

Smart Contracts

*Qué son, para qué sirven
y para qué no servirán*

Autor

Mag. Sebastián Heredia Querro

SMART CONTRACTS

*QUÉ SON, PARA QUÉ SIRVEN Y PARA QUÉ NO
SERVIRÁN*

Mag. Sebastián Heredia Querro

**Universidad Católica de Córdoba
Centro de Emprendedorismo e Innovación
CEINN-UCC**

2020



Heredia Querro, Sebastián

Smart contracts : qué son, para qué sirven y para qué no servirán /
Sebastián Heredia Querro ; prólogo de Federico Ast. - 1a ed. -
Ciudad Autónoma de Buenos Aires : IJ Editores, 2020.
Libro digital, EPUB

Archivo Digital: descarga y online
ISBN 978-987-8377-31-5

1. Derecho. I. Ast, Federico, prolog. II. Título.
CDD 346.02

Las posturas doctrinarias expresadas en los artículos
aquí incluidos son de exclusiva responsabilidad de sus autores
y no necesariamente reflejan los puntos de vista de la Editorial,
la Institución, el Director ni del Comité Editorial.

Se prohíbe la reproducción total o parcial
de esta obra sin la autorización expresa.

IJ International Legal Group
Dirección y correspondencia: Lavalle 1115 - PB,
Ciudad Autónoma de Buenos Aires, Argentina
CP: 1048
TE: +54 011 5276-8001

Derechos reservados por la Ley N° 11.723

Índice

A. Caveat lector

I. Objetivos de este Manual

II. Alcance del este Manual

III. Errores de este Manual

IV. Ausencia de conflicto de interés

V. Recursos electrónicos no permanentes

VI. Idioma inglés

VII. Uso (extensivo) de las notas al pie

B. El (gran) impacto de la *Blockchain* en el Derecho (y viceversa)

I. Blockchain: FAQs

1.1. Blockchain

1.1.1. Cypherpunks

1.1.2. El avance tecnológico y la Riqueza de las Redes

1.1.3. From Internet of Information to Internet of Value y a la criptoconomía

1.1.3.1. La pizza más cara de la historia

[1.1.4. Antes de Bitcoin: BitGold](#)

[1.1.5. Reeditando viejas discusiones \(de cuando irrumpió Internet\)](#)

[1.1.6. Blockchain vs. DLTs vs. Sistemas Distribuidos](#)

[1.1.7. Algunas definiciones \(y un ejemplo clásico para ilustrar su funcionamiento\)](#)

[1.1.8. Características esenciales de la blockchain](#)

[1.1.8.1. Decentralización](#)

[1.1.8.2. Mecanismos de consenso](#)

[1.1.8.2.1. Protocolos de consenso](#)

[1.1.8.2.2. Cambios en el protocolo](#)

[1.1.8.2.3. Registro inmutable \(¿y GDPR?\)](#)

[1.1.9. Tipos de blockchains](#)

[1.1.9.1. Abiertas](#)

[1.1.9.1.1. El riesgo operacional de las blockchains públicas](#)

[1.1.9.1.2. El \(supuesto\) riesgo del autoritarismo on-chain](#)

[1.1.9.2. Privadas](#)

[1.1.9.3. Híbridas](#)

[1.1.9.4. Otras clasificaciones](#)

[1.1.10. La evolución de la Blockchain](#)

[1.1.11. Grupos de interés](#)

[1.1.12. Inversiones en blockchain en 2019](#)

[1.2. Limitaciones de la *Blockchain*](#)

[1.3. Cryptocurrency & Blockchain 1.0](#)

[1.3.1. El Cryptomarket](#)

[1.3.2. CBDCs](#)

[1.3.3. Libra](#)

II. Smart Contracts: FAQs

[2.1. Algunas definiciones \(*fans vs. haters*\)](#)

[2.1.1. Clasificación de los contratos inteligentes](#)

[2.1.2. Naturaleza jurídica de los contratos inteligentes](#)

[2.1.3. Contratos inteligentes y el ejercicio de la profesión de Abogado](#)

[2.1.4. Smart Contracts vs. Computable Contracts](#)

[2.1.4.1. Términos contractuales computables](#)

[2.1.4.2. Limitaciones de los data-oriented contracts](#)

[2.1.4.3. Otras limitaciones y beneficios](#)

[2.1.5. La visión de Samuel Bourque](#)

[2.2. Cuatro pilares fundamentales de los *Smart Contracts*](#)

[2.2.1. Observabilidad: el regreso de la Pitonisa \(reloaded\) y los Oráculos](#)

[2.2.2. Verificabilidad](#)

[2.2.3. Privacidad \(efecto relativo 2.0 +/- identidad +/-](#)

confidencialidad +/- anonimidad)

2.2.3.1. Anonimidad y pseudonimidad en la blockchain: encriptado asimétrico y On-Chain Analytics

2.2.3.1.1. Llave pública y billeteras digitales – Wallets

2.2.4. Ejecutabilidad (o cumplimiento forzoso o automatizado).

2.3. Usos actuales de Smart Contracts. Smart Contracts híbridos

2.4. Desmitificando a los *Smart Contracts*

2.4.1. Creación de tokens vs. transferencia de tokens vía Smart Contracts

2.4.2. Codificación deficiente o inexacta de un Smart Contract

2.4.3. Traducción del lenguaje natural: sus limitaciones

2.4.4. Codificación directa de obligaciones contractuales

2.4.5. Criminal Smart Contracts

2.4.6. Problemas para la ejecución judicial de Smart Contracts

2.5. Juez competente, ley aplicable y resolución de controversias en un entorno de *blockchain-based Smart Contracting*

2.5.1. Justificantes de una Jurisdicción Distribuida

2.5.2. Características de una Jurisdicción Distribuida

2.5.3. Casos de uso. Say (again) hello to Ricardian contracts!

2.6. Dapps, DOs, DAOs y DACs

2.6.1. Round 1: Enter The DAO

2.6.1.1. El Caso TheDAO

2.6.1.1.1. Responsabilidad de los inversores y desarrolladores

2.6.1.1.2. Naturaleza jurídica de la participación societaria

2.6.1.1.3. Status legal de una DAO: una propuesta de lege ferenda

2.6.3. DAOs, DACs e Internet of Things

2.6.3. Round 2: Enter The LAO (DAOs 2.0!)

2.6.3.1. Ragequit, o el derecho de receso digital en el Siglo XXI

2.7. Haciendo marcha atrás con un *Smart Contract*: ¿Se puede?

2.7.1. Token propio

2.7.2. ¿Contrato reversible?

2.8. Hacia la estandarización de *Smart Contracts*

III. Tokens & *Smart Contracts* vs. La Ley

3.1. La declaración de independencia del Ciberespacio

3.2. Tres (posibles) formas de interacción entre la Blockchain y el Derecho

3.2.1. Evasión hostil

3.2.1.1. SilkRoad

3.2.1.2. Ripple

3.2.1.3. La regulación de China sobre Bitcoin y blockchain

3.2.2. Alineación eficiente

3.2.2.1. Corda (R3)

3.2.2.2. Suplementar, complementar o sustituir

3.2.3. Aliviar fricciones transaccionales

3.2.3.1. Crowdfunding vía ICOs, STOs, DAICOs & IEOs. Reenvío a taxonomía del Token.

3.2.3.2. Generación eléctrica distribuida

3.2.4. Good Blockchain Governance

3.3. Tokens vs. Law: perspectivas en el derecho comparado

3.3.1. Taxonomía del Token

3.3.1.1. Primeros acercamientos regulatorios y legislativos. Token Taxonomy Act de 2019.

3.3.1.2. Security Token Offering (STO)

3.3.1.2.1. Simple Agreement for Future Token (SAFT)

3.3.1.3. Initial Coin Offerings: Soft Cap y Hard Cap

3.3.1.4. Tokens: substance over form, STOs vs. ICOs.

3.3.1.5. Cuando la claridad regulatoria es necesaria

3.3.5.1.1. Precisiones terminológicas

3.3.5.1.2. Proceso de venta de App Tokens

3.3.5.1.3. El régimen federal de títulos valores regulados en EE.UU.

3.3.5.1.4. Factores intrínsecos y extrínsecos

3.3.1.6. DAICOs y IEOs

3.3.2. Tokenización

3.3.2.1. Sus beneficios

3.3.2.1.1. Comercialización de valores negociables

3.3.2.1.2. Pricing de valores negociables

3.3.2.1.3. Post-trade

3.3.2.1.4. Desintermediación relativa

3.3.2.2. Tokenización de Valores Negociables

3.3.2.3. Tokenización: ¿la nueva Securitización?

3.3.2.4. Tokenización Inmobiliaria

3.3.2.5. Riesgos y desafíos

3.4 Criptoactivos y *Smart Contracts*: perspectiva comparada

3.4.1. Reino Unido

3.4.1.1. Principio de Neutralidad Tecnológica y FCA Innovate

3.4.1.1.1. Regulatory Sandbox

3.4.1.1.1.1. Otros países que siguen el modelo

SandBox

3.4.1.2. Lineamientos de la FCA sobre criptoactivos

3.4.1.3. LawTech Delivery Panel y la UK Jurisdiction Taskforce (UKJT)

3.4.1.3.1. Características d los criptoactivos

3.4.1.3.1.1. Autenticación vía encriptación

3.4.1.3.1.2. Uso de un registro distribuido de transacciones

3.4.1.3.1.3. Protocolo de gobierno

3.4.1.3.1.4. Transferencia vs. Gasto & Doble Gasto

3.4.1.3.1.5. Son una propiedad

3.4.1.3.1.6. Criptoactivo como garantía convencional

3.4.1.3.1.7. Criptoactivos vinculados a bienes off-chain

3.4.1.3.2. Smart Contracts

3.4.1.3.2.1. La forma de los contratos en el Derecho Inglés. Interpretación de un contrato

3.4.2. Estados Unidos de Norteamérica

3.4.2.1. Empresas que operan criptoactivos

3.4.2.2. Admisión y utilización de la blockchain a nivel federal y estadual

3.4.2.2.1. Admisión expresa de los contratos inteligentes a nivel estadual

3.4.2.2.2. Regulación de la blockchain a nivel estadual

3.4.2.2.3. The Crypto-currency Act of 2020

3.4.3. Singapur

3.4.3.1. Tokens regulados

3.4.3.2. Tokens no regulados. SandBox

3.4.4. Suiza

3.4.4.1. FINMA

3.4.4.2. La Swiss LegalTech Association (SLTA): su posicionamiento en contratos inteligentes

3.4.5. España

3.4.5.1. Legislación aplicable

3.4.5.1.1. ¿Son contratos en sentido legal?

3.4.5.1.1.1. Objeto, causa y consentimiento del contrato

3.4.5.1.1.2. Forma del contrato

3.4.5.1.2. Proceso de formación del contrato inteligente

3.4.5.1.3. El error en la formación de contratos inteligentes

3.4.5.1.4. La prueba del contrato en juicio

3.4.5.1.5. El pago en los contratos inteligentes

3.4.6. Japón

3.4.6.1. Informe del Grupo de Estudios de los Servicios de Cambio de Monedas Virtuales

3.4.6.1.1. Nueva definición de criptoactivos

3.4.6.1.2. Servicio de custodia de criptoactivos

3.4.6.1.3. Regulación de los Exchanges

[3.4.6.1.4. Electronically recorded transferable rights \(ERTRs\)](#)

[3.4.6.1.5. Derivados sobre criptoactivos](#)

[3.4.6.1.6. Actos desleales con criptoactivos](#)

[3.4.6.2. Informe del Ministerio de Economía, Comercio e Industria de Japón](#)

[3.4.7. Corea del Sur](#)

[3.4.8. Francia](#)

[3.4.8.1. Registro voluntario de utility tokens. Definición de propiedad](#)

[3.4.8.2. Tratamiento de los security tokens. Propuesta de SandBox europeo. Modificaciones requeridas](#)

[3.4.8.2.1. Casos de STOs franceses](#)

[3.4.8.2.2. Prospectos de emisión e intermediarios](#)

[3.4.8.2.3. Know Your Customer/Client. Restricciones a la transferencia](#)

[3.4.8.2.4. Plataformas de trading de STOs](#)

[3.4.8.3. Registro voluntario de DASPs. Registro obligatorio](#)

[3.4.9. México](#)

[3.4.9.1. Activos virtuales, Exchanges y Wallets](#)

[3.4.9.2. Información al usuario de activos virtuales](#)

[3.4.9.3. SandBox](#)

[3.4.9.3.1. Modelos novedosos](#)

3.4.9.3.2. Autorizaciones temporales. Condiciones para su concesión

3.4.9.3.3. Operaciones de entidades financieras con activos virtuales

3.4.9.3.4. Obligaciones por la concesión de autorizaciones temporales

3.4.10 Chile

3.4.10.1. El Tribunal de Defensa de la Libre Competencia y los criptoactivos

3.4.10.2. La posición de la Corte Suprema de Justicia de Chile

3.5. Criptoactivos & *Smart Contracts* vs. Derecho Nacional: *Lege Data y Lege Ferenda*

3.5.1. Criptoactivos, Contratos Inteligentes y Código Civil y Comercial de la Nación (CCCN)

3.5.1.1. Los criptoactivos como documento digital con firma electrónica

3.5.1.2. Los criptoactivos como un bien

3.5.1.2.1. Definición de bien para el derecho argentino

3.5.1.2.2. El objeto de los derechos reales

3.5.1.2.3. Derechos reales sobre cosas registrables

3.5.1.2.4. Los criptoactivos como un commodity

3.5.1.2.5. Los criptoactivos son un bien mueble incorporal registrable

3.5.1.3. ¿Los criptoactivos como un título valor no

cartular atípico?

3.5.1.3.1. Libertad de creación de títulos valores: causales vs. Abstractos

3.5.1.3.2. Los criptoactivos como valores negociables

3.5.1.3.3. Utility y Security tokens vs. Ley de Mercado de Capitales

3.5.1.3.3.1. La regulación del Equity crowdfunding en Argentina

3.5.1.3.3.1.1. Plataformas de financiamiento colectivo. Administración y fiscalización

3.5.1.3.3.1.2. Capital social y patrimonio neto mínimo. Contratos. Sistemas

3.5.1.3.3.1.3. Guía de selección de Proyectos. Advertencia al inversor y derecho a retractarse. Prohibiciones

3.5.1.3.3.1.4. Identificación de ofertas: transparencia. Comisiones

3.5.1.3.3.1.5. Instrumentos de inversión. Mercado secundario. Monto máximo de emisión y de inversión

3.5.1.3.3.1.6. Información sobre el Proyecto de Financiamiento Colectivo. Cambio material en el Proyecto

3.5.1.3.3.1.7. Importancia del Equity Crowdfunding

3.5.1.3.3.1.8. Quid de la aplicabilidad de la regulación del equity crowdfunding a los Security Token

3.5.1.4. Blockchain Federal Argentina (BFA): BaaS

3.5.1.4.1. Miembros de BFA. Modelo participativo e ingeniería organizacional

3.5.1.4.2. Almacenamiento off-chain

3.5.1.5. Contratos inteligentes: su recepción legal en Argentina

3.5.1.5.1. Contratos inteligentes como contratos electrónicos

3.5.1.5.2. El contrato inteligente como contrato celebrado por adhesión

3.5.1.5.2.1. El contrato adhesivo

3.5.1.5.2.2. Requisitos de las cláusulas generales predispuestas

3.5.1.5.2.3. Interpretación del contrato por adhesión

3.5.1.5.2.4. Cláusulas particulares en el contrato por adhesión

3.5.1.5.2.5. Cláusulas abusivas en el contrato por adhesión

3.5.1.5.2.6. Problemática del contrato inteligente como contrato adhesivo

3.5.1.6. Es interesante también analizar el reflejo contable de los criptoactivos y del efecto de sus transacciones mediante contratos inteligentes. La materia, en éste ámbito como en otros, se está desarrollando rápidamente.

3.5.1.6.1. Criptomonedas

[3.5.1.6.2. Taxonomía del token y opciones de reflejo contable](#)

[3.5.1.6.2. Utility tokens](#)

[3.5.1.6.3. Asset tokens](#)

[3.5.1.6.4. Security tokens](#)

[3.5.1.6.5. Tokens híbridos](#)

[3.5.1.7. Contratos Inteligentes vs. Estatuto del Consumidor](#)

[3.5.1.7.1. ¿Beneficios para los consumidores?](#)

[3.5.1.7.2. Constitución Nacional, CCCN, ley especial y otras normas tuitivas](#)

[3.5.1.7.3. Definición de consumidor o usuario. Airdrops](#)

[3.5.1.7.4. Proveedor de contratos inteligentes, o que utiliza contratos inteligentes](#)

[3.5.1.7.5. Información y publicidad en materia de contratos inteligentes](#)

[3.5.1.7.6. Riesgos derivados del uso de contratos inteligentes en la comercialización de bienes y servicios. Facultad de revocación](#)

[3.5.1.8. Blockchains, Contratos Inteligentes vs. Defensa de la Competencia. Efectos de Red vs. Efectos del Token](#)

[3.5.1.8.1. Id quod plerumque accidit](#)

[3.5.1.8.2. La definición de mercados relevantes on-chain](#)

[3.5.1.8.3. Conductas anticompetitivas unilaterales on-chain](#)

[3.5.1.8.4. Colusión mediante contratos inteligentes](#)

[3.5.1.8.5. Cinco principios esenciales que deben ser tenidos en cuenta al regular la blockchain](#)

[3.5.1.8.5.1. Pseudonimidad como característica esencial](#)

[3.5.1.8.5.2. Arquitectura distribuida](#)

[3.5.1.8.5.3. Transmisión peer-to-peer entre usuarios](#)

[3.5.1.8.5.4. Protocolos de consenso](#)

[3.5.1.8.5.5. Inmutabilidad](#)

[3.5.1.9. Contratos Inteligentes vs. Régimen Falencial](#)

[3.5.1.9.1. El Derecho Concursal. Principios. Procesos. Cesación de pagos](#)

[3.5.1.9.2. Efectos del concurso preventivo y la quiebra](#)

[3.5.1.9.3. Contratos con prestaciones recíprocas pendientes, facultad resolutoria y reglas para algunos contratos en particular](#)

[3.5.1.9.4. Quiebra y desapoderamiento. Activos intangibles en el régimen falencial](#)

[3.5.1.9.5. Acciones de recomposición patrimonial](#)

[3.5.1.9.6. Smart Contracs vs. LCQ](#)

[3.5.1.10. Contratos Inteligentes vs. Régimen de Protección de Datos Personales](#)

[3.5.1.10.1. Derecho al olvido: ¿Un derecho a borrar?](#)

[3.5.1.10.2. Decisiones basadas únicamente en el tratamiento automatizado de datos](#)

3.5.1.10.3. General Data Protection Regulation

3.5.1.10.3.1. Alcance de la GDPR

3.5.1.10.3.2. GDPR vs. Blockchains: derecho a rectificar los datos y derecho al olvido

3.5.1.10.4. Smart Contracts, derecho al olvido, decisiones basadas en datos, y otra tecnología en ascenso: Enter the Machine Learning (una disgresión)

3.5.1.10.4.1. Algunas precisiones en cuanto al uso de los términos

3.5.1.10.4.2. Descripción, predicción y prescripción

3.5.1.10.4.3. Breve historia de la Inteligencia Artificial. La Singularidad

3.5.1.10.4.4. Inteligencia Artificial vs. Machine Learning

3.5.1.10.4.5. El Data Scientist

3.5.1.10.4.6. El impacto laboral de la IA

3.5.1.10.4.7. Explainability

3.5.1.10.4.8. El Gobierno del Dato y el Feature Engineering

3.5.1.10.4.9. Problemas de regresión y problemas de clasificación

3.5.1.10.4.10. Unsupervised Machine Learning

3.5.2. Criptoactivos, Contratos Inteligentes & Lege Ferenda: Análisis y crítica de legislación proyectada en Argentina

IV. Cuestiones Contractuales, Judiciales y Responsabilidad Civil Emergente

4.1. Introducción

4.2. La conexidad contractual

4.2.1. Clases y modalidades de contratos conexos

4.2.2. Efectos e interpretación de los contratos conexos

4.2.2.1. Excepción de incumplimiento contractual. Suspensión de cumplimiento

4.2.2.2. Frustración de la finalidad económica común

4.2.2.3. Resolución por incumplimientos conexos

4.2.2.4. Deberes de cooperación y de conducta. Deberes respecto de “terceros”

4.2.2.5. Extensión de la responsabilidad

4.2.2.6. Interpretación de contratos conexos

4.3. contrato para programar un *Smart Contract*: Aspectos controvertidos

4.3.1. Especificaciones y funcionalidades a cumplir por el Smart Contract. Arquitectura del software

4.3.2. El Decreto 165/1994 del Poder Ejecutivo de la Nación

4.3.3. Recepción de la obra

4.3.4. Responsabilidad de la empresa (equipo) de

programación (contratista)

4.3.5. Aspectos controvertidos del desarrollo y la comercialización del software

4.4. Proveedor de servicios de auditoría técnica de *Smart Contracts*

4.4.1. Proceso de auditoría

4.4.2. Productos imperfectos pero perfectibles

4.4.3. El contrato de auditoría técnica de un Smart Contract

4.4.4. Empresa de programación que ofrece servicios de auditoría

4.4.5. Pago al auditor

4.4.6. Prestación de servicios de auditoría y Estatuto del Consumidor

4.5. Proveedor de servicios de Exchange, Trading y Billetera Digital

4.5.1. Exchanges

4.5.2. KYC & AML

4.5.3. Monedas virtuales “sospechosas” y listas negras

4.5.4. Relaciones contractuales en el ámbito de los Exchanges

4.5.5. Ciberataques a los Exchanges: una tendencia preocupante

4.5.6. Litigio colectivo, Exchanges y trading platforms

4.5.7. El caso B2C2 vs. Quoine Pte Ltd.

4.5.7.1. El caso Coinzest

4.5.8. Wallets

4.5.9. ¿Licencia de software o depósito de información?

4.5.10. Términos y condiciones de un contrato de licencia de Wallet software

4.5.10.1. El licenciatario de software como usuario protegido por el Estatuto del Consumidor

4.5.11. Hot & Cold Wallets y MultiSig Wallets

4.5.12. Ataques a Wallets

4.5.13. La regulación argentina de las billeteras digitales. Los Proveedores de Servicios de Pago y el Dinero electrónico

4.5.13.1. El auge de los procesadores de servicios de pago

4.5.13.2. El fenómeno Mercado Pago

4.5.13.3. La Comunicación “A” 6859

4.5.13.4. La Comunicación “A” 6885

4.5.13.5. El ecosistema Fintech argentino

4.5.13.6. Marcos regulatorios de los ecosistemas Fintech: el proyecto de SandBox español

4.5.13.7. Hacia el Open Banking

4.5.13.8. Situación de los Exchanges de criptoactivos: ¿son PSPs?

4.6. Dinámicas (contractuales) de Creación,

Estandarización, Comercialización y Adquisición de Tokens

4.6.1. Protegiendo al adquirente de tokens digitales a través del Legal Design

4.7. Responsabilidad de las plataformas de *blockchain*

4.7.1. El Derecho Privado ante la blockchain

4.7.2. Responsabilidad objetiva en entornos de blockchain

4.7.3. Las cláusulas del liberación de responsabilidad

4.7.4. Seguro obligatorio de responsabilidad civil

4.7.5. El enfoque norteamericano

4.7.5.1. ¿Hard cases make bad law? el caso SEC v. Shavers

4.7.5.2. El caso Munchee, Inc.

4.7.5.3. El caso SEC v. AriseBank

4.7.5.4. El caso CFTC v. McDonnell

4.7.5.5. El caso Skatteverket v. Hedqvist

4.7.6. La responsabilidad por riesgo: la teoría del riesgo creado

4.7.6.1. El riesgo como factor de atribución de responsabilidad

4.7.7. Fundamento de la responsabilidad por riesgo

4.7.8. Actividades riesgosas

4.7.9. Beneficiario de la actividad riesgosa

4.7.10. Eximentes de responsabilidad

4.8. Primeras reflexiones preliminares en torno a la responsabilidad civil en entornos de *blockchain*

4.8.1. Los Usuarios de la Innovación y los Creadores de la Innovación

4.8.2. Redes contractuales dentro de redes digitales

4.8.3. Responsabilidad objetiva, seguros y cláusulas de limitaciones de responsabilidad en entornos blockchain

4.8.4. Taxonomía del token y asignación de riesgos

4.8.5. Responsabilidad de los actores periféricos e internos: Exchanges, Wallets y desarrolladores de Smart Contracts

4.8.6. Blockchains privadas y consorciadas

4.8.7. Innovación y Competencia

V. Aspectos Regulatorios y Tributarios

5.1. Introducción. Primeros pasos hacia el entorno *blockchain* en Argentina

5.2. Breve descripción de los mercados de dinero *fiduciario* regulados en Argentina

5.2.1. Bancos, compañías financieras y proveedores no financieros de crédito

5.2.2. Algunas innovaciones jurídicas en la financiación del capital de trabajo: el cheque y el pagaré bursátil. El cheque electrónico y la factura de crédito electrónica

5.2.2.1. La negociación bursátil de cheques de pago diferido

5.2.2.2. El pagaré bursátil

5.2.2.3. El cheque electrónico y la factura de crédito electrónica

5.2.3. Funcionamiento e instituciones del mercado de capitales argentino

5.2.3.1. El rol de la Comisión Nacional de Valores

5.2.3.2. La oferta pública de títulos valores, la contratación bursátil y los intermediarios bursátiles

5.2.3.3. Algunas innovaciones jurídicas en el mercado de capitales argentino

5.2.3.3.1. Regulación de los contratos derivados

5.2.3.3.2. Desmaterialización de títulos valores con oferta pública

5.2.3.3.3. Hacia los bonos verdes on-chain: los G-ABS.

5.2.3.3.3.1. Acelerar las Finanzas Climáticas

5.2.3.3.3.2. Los Valores Negociables SVS

5.2.3.3.3.3. Estímulo Fiscal

5.2.3.3.3.4. Green Blocks: kickstarting the blockchain-based green bonds Industry

5.2.3.3.3.5. Bond-i: el Canguro disruptivo

5.2.3.3.3.6. El primer bono verde emitido en blockchain

5.2.3.3.3.7. On-chain payments: StableCoins y Central

Bank Digital Currencies

5.2.3.3.3.8. Pruebas de Impacto: off-chain vs. on-chain + real time + on line

5.2.3.3.3.9. Trazabilidad en la utilización de fondos

5.2.3.3.3.10. Nodos para supervisores bursátiles

5.2.3.3.3.11. La imperiosa necesidad de democratizar la inversión de impacto alineada a los ODS

5.3. Avances regulatorios: perspectiva comparada

5.3.1. Commodities vs. ICOs vs. STOs

5.3.1.1. Directrices sobre token sales de la SEC

5.3.1.2. IOSCO y las plataformas de trading de criptoactivos

5.3.1.3. Directrices de la Financial Crimes Enforcement Network (FinCEN)

5.3.1.4. La auto-regulación de los intermediarios: Financial Industry Regulatory Authority (FINRA)

5.3.1.5. Commodity Futures Trading Commission (CFTC)

5.3.1.5.1. CFTC vs. Coinflip

5.3.1.6. El caso de Malta

5.3.1.6.1. Utility tokens

5.3.1.6.2. Activo Financiero Virtual

5.3.1.6.3. El SandBox maltés: gaming & gambling meets the ledger

5.3.1.7. Otros enfoques regulatorios

5.4. Aspectos fiscales: perspectiva comparada. Tributación en Argentina.

5.4.1. La tributación digital

5.4.2. Breve perspectiva comparada de la tributación de los criptoactivos

5.4.3. La tributación de los criptoactivos en Argentina

5.5. ¿Elaboración Participativa de Normas?

VI. Casos de Uso en el Mundo de los Negocios. Smart Citizens

6.1. *Blockchains y Smart Contracts*: Casos de uso en el Mundo de los Negocios.

6.1.1 RegTech

6.1.2. Energía

6.1.3. Comercio Internacional

6.1.4 Industria automotriz

6.1.5. Industria aeronáutica

6.1.6. Mercados bancarios y financieros

6.1.7. Real Estate

6.1.8. Health Care

6.1.9. Supply Chain Management (SCM)

[6.1.10. Industria del Seguro](#)

[6.1.11. Registros marcarios](#)

[6.1.12. Gestión de derechos digitales](#)

[6.1.13. Publicidad digital](#)

[6.1.14. Certificados académicos](#)

[6.1.15. Arte y Blockchain](#)

[6.1.16. Gestión del talento humano](#)

[6.1.17. Blockchain y crisis humanitarias ¿Blockchain en los ojos?](#)

[6.2. Smart Citizens](#)

[6.2.1. Voto y Blockchain](#)

[6.2.2. Participación ciudadana on-chain: el caso Alcobendas](#)

[6.2.3. Compras públicas on-chain](#)

[6.2.4. Registros inmobiliarios](#)

[6.2.5. Blockchain y cobro de impuestos](#)

[6.2.6. Homeless ID: el caso de Texas](#)

VII. Uniendo Los Puntos

[7.1. Convertir la *Información en Conocimiento*](#)

[7.2. Una obligación *moral y ética*](#)

[7.3. Aceleración](#)

A mi Madre, *Liliana G. Querro de Luna*,
que dio su vida al servicio de la Justicia

“La confianza es un sustituto imperfecto de la información”
POSNER, Richard, “The right of privacy”, 12 *Ga. L. Rev.* 393 (1978)

Ad augusta per angosta

(Monse 2001)

Veritas liberabit vos

*“We tend to overestimate the impact of technologies in the short run but
underestimate them over the long term”*

Amara's Law

Prólogo a la primera edición

A comienzos del siglo XIX, el filósofo Jeremy Bentham se embarcó en una cruzada por la codificación del derecho. Quería transformar la ley oral en código escrito. Su sueño era compilar todas las leyes del mundo en un gran libro. Se trataba, para él, de un requisito básico para el acceso a la justicia.

La tradición oral era poco clara y subjetiva, lo que dejaba un amplio espacio para arbitrariedades y manipulaciones de jueces y abogados inescrupulosos. La ley escrita era (más) clara y (más) objetiva. En su cruzada, Bentham ofreció a los gobiernos de Estados Unidos, Rusia y España, entre otros, codificar sus leyes orales.

El siglo XIX fue el siglo de la codificación. Los códigos legales escritos ofrecieron garantías de previsibilidad y derechos de propiedad para el despegue de la revolución industrial y el ascenso del capitalismo a escala global. Fueron también pilares que protegieron los derechos de los individuos contra los gobiernos.

A comienzos del siglo XXI, sin embargo, el paradigma bajo el que se construyó el sueño de Bentham empieza a alcanzar sus límites. El advenimiento de Internet trajo un cambio radical en la forma de conectarnos y hacer negocios. Las interacciones son inmediatas y globales. Ya no respetan los tiempos ni los límites jurisdiccionales de los códigos creados en la era de la imprenta y los estados nacionales.

El desafío de nuestra época es construir la estructura jurídica para la sociedad digital y la cuarta revolución industrial. Una economía en la que personas de todo el mundo pueden colaborar con su trabajo y capital de un modo que nunca antes había sido posible.

La nueva realidad económica y social requiere una nueva tecnología de acuerdos. En 1996, el criptógrafo Nick Szabo propuso el concepto de *contratos inteligentes* como una nueva tecnología jurídica para la era de los mercados digitales. Estos contratos, escritos en código informático, tienen la propiedad de autoejecutarse cuando se cumplen las condiciones establecidas. En 2008, una persona (o grupo de personas) bajo el seudónimo de Satoshi

Nakamoto propuso el *blockchain*, una tecnología de base de datos compartida y abierta.

La combinación de estas tecnologías trae la promesa de una nueva estructura jurídica para la sociedad digital: contratos que se autoejecutan de manera automática e inmediata en redes globales seguras y descentralizadas. El desafío de codificación de nuestro tiempo es la construcción de lo que se conoce como la *Lex Cryptographia*, un sistema legal construido sobre código de computadora y seguridad criptográfica que nadie puede manipular. Del código en lenguaje natural al código en lenguaje de computadora.

Este libro ofrece una enorme contribución a la comprensión y difusión de los contratos inteligentes y su impacto sobre el futuro del derecho. Brinda al lector un panorama muy amplio sobre el *blockchain*, criptoactivos, aplicaciones descentralizadas, y como todo esto interactúa con el paradigma legal tradicional.

Como dice el experto en innovación en derecho, Richard Susskind: la industria legal sufrirá mayores cambios en los próximos 20 años que en los últimos 200.

Este libro brinda un amplio panorama importante de esta transformación. Una nueva fase del sueño de Bentham: la codificación del derecho para la era de Internet.

Federico Ast

Buenos Aires, 30 de mayo de 2020

A. Caveat lector

I. Objetivos de este Manual

Esta obra tiene un modesto objetivo: ser un manual para uso y consulta, principalmente, por parte de estudiantes y profesionales del mundo del Derecho, sin que ello precluya a otras partes interesadas la posibilidad de adentrarse al mundo del *blockchain* y los *Smart Contracts* mediante su lectura. El interés es la medida de la acción, y comenzar, de a poco, a entender cómo funcionan las tecnologías de registro distribuido, las cadenas de bloques y los *Smart Contracts* beneficiará a todo aquél que emprenda el viaje que se propone en esta obra, sea o no profesional del Derecho.

Si el declarado objetivo llega a ser cumplido exitosamente, el lector habrá salido del estado de *ceguera cognitiva* en el que previamente se encontraba, es decir, de aquél estado en el cual *no se sabe todo lo que no se sabe*.

II. Alcance del este Manual

El modesto objetivo de este Manual delinea y condiciona su alcance. Probablemente no encontrará aquí el lector todas las respuestas a todas sus dudas e inquietudes generadas por la irrupción de la cadena de bloques o los contratos inteligentes. Es más, lamento informar que probablemente se generen más dudas, más preguntas, y tan solo unas pocas certezas.

Desde ya, adviértase que la presente obra aspira a ser una mera recopilación –previa traducción propia, en muchos casos– de los *papers* y noticias más relevantes en la materia, ordenados de modo tal que se facilite su digestión. No se encontrará aquí, salvo pocas excepciones, ninguna innovación, ninguna disrupción, sino una humilde sistematización de ideas e innovaciones ajenas.

III. Errores de este Manual

Advierta el lector que este Manual ha sido escrito por un abogado, sin conocimiento alguno de programación, y no ha sido revisado por ningún

idóneo de la programación, con lo cual es (muy) probable que existan muchas inexactitudes (o, directamente, errores) desde el punto de vista de la ciencia de la programación. Hasta donde mi capacidad y formación lo permiten, no he encontrado errores o inconsistencias evidentes o groseras. Se agradece al lector enviar aviso en caso de detectar algún error o inconsistencia grosera.

IV. Ausencia de conflicto de interés

El autor declara que ninguna organización, empresa o grupo de interés vinculado a, con conexión directa o indirecta con, o con negocios actuales o futuros vinculados a, la cadena de bloques y a los contratos inteligentes ha financiado o aportado recursos de índole alguna para la elaboración del presente Manual. Los sesgos ideológicos o argumentativos, en caso de existir, son de exclusiva propiedad del autor y de ninguna otra persona u organización.

V. Recursos electrónicos no permanentes

El autor declara que para la redacción de este Manual se ha recurrido a muchos recursos bibliográficos electrónicos (más de 4000 *links* a websites), todos ellos accesibles entre abril y mayo de 2020, pero cuya accesibilidad posterior el autor no puede garantizar.

VI. Idioma inglés

Por razones de claridad expositiva en la *fuentes*, el autor quiere justificar la cita textual de frases y extractos en idioma inglés en varios capítulos de este Manual y en sus notas al pie. Allí donde ha sido conveniente, se han realizado traducciones libres al idioma castellano, pudiendo existir errores de traducción, por los cuales se ofrecen las disculpas del caso por adelantado.

VII. Uso (extensivo) de las notas al pie

Finalmente, el autor quiere justificar anticipadamente el uso extensivo de notas al pie, toda vez que este manual no supera las 600 páginas pero tiene casi 3000 notas al pie. La razón es, principalmente, un sesgo personal: siempre he juzgado a los libros que leo en función de las notas al pie *hacia otros* autores, además de por su contenido, obviamente. Considero que muchas citas enriquecen la transferencia de conocimiento, pero con una particularidad: generalmente la nota amplía un concepto, o presenta un concepto *distinto*, pero *vinculado* al que se trata en el texto del Manual. Yo las he usado para ambos fines: ampliar y vincular. Hay información muy valiosa en las notas, por lo que se recomienda al lector la lectura de las mismas, aunque lo importante, lo esencial, estará siempre contenido en el texto, y no en sus notas al pie.

B. El (gran) impacto de la *Blockchain* en el Derecho (y viceversa)

Es importante que los profesionales del Derecho comiencen a acercarse a la *blockchain*, para conocer y entender sus potencialidades, y también sus limitaciones.

El FORO ECONÓMICO MUNDIAL afirma que en 2027 el 10% del Producto Bruto Global estará *almacenado* en *blockchains*^[1], y según GARTNER será un mercado de servicios de un valor aproximado de 3.1 Trillones de Dólares en 2030; ya será un mercado de 1.5 Trillones de Dólares dentro cinco años^[2]. Para ponerlo en términos relativos, y asumiendo un PBI de Argentina de 519 mil millones de Dólares (2018), la tecnología de las cadenas de bloques –a.k.a. *blockchains*– podrían –en tan solo 10 años– crear un nuevo mercado con un tamaño equivalente a seis veces el PBI argentino. Va de nuevo: 6 PBIs. Tan considerable creación de valor no debiera gestarse y desarrollarse sin un acompañamiento legal que la enriquezca y le aporte un reparto de riesgos eficiente. Pero cuidado: es necesaria una gran cuota de *Astucia Legal*^[3] para navegar aguas turbulentas, bajo la guía de la brújula de las cuatro innovaciones incrementales –algunas fundacionales, otras experimentales– que están en su infancia o adolescencia, pero que madurarán en la próxima década, y se combinarán en modos que aún no hemos diseñado. Me refiero a la Inteligencia Artificial, el *Blockchain*, el *Internet of Things* –incluyendo el *Industrial Internet of Things*, *IIoT*– y la Computación Cuántica. En este sentido, empiezan ya a pensarse combinaciones entre Inteligencia Artificial y *Blockchain*, que permiten dejar registrado en *blockchain* el proceso de aprendizaje de los algoritmos, de modo tal de poder

rápidamente detectar errores en el entrenamiento de algoritmos^[4].

En palabras de Alegría^[5], nuestra cultura jurídica no sólo no puede quedar encandilada por grandes luces, sino que está encomendada a usar el ingenio para recibir y mejorar lo que se decante de precedentes computables, debiendo desarrollar la *ars combinatoria* que requiere de una inventiva propia, de una generación de nuevos recursos técnicos que sirvan para nuestras comunidades en el actual estado de su desarrollo.

Pero, ¿qué tiene de potencial un sistema de “libros contables” i.e. bases de datos distribuidas –Fray Luca Pacioli alucina desde el Paraíso Contable–, accesible generalmente por cualquier persona, que almacena información “agrupada” en forma de “cadenas de bloques” y que –extrañamente, en un mundo dinámico–, son generalmente “inmutables” y “ordenadas cronológicamente” y sólo permiten agregar información bajo ciertos “acuerdos” predeterminados?^[6]

A responder esta pregunta se dedica este Manual, pero es importante introducir, *ab initio*, algunos ámbitos^[7] en los que al momento presente (abril 2020) la *blockchain* ya está impactando de lleno en la forma de ejercer la profesión legal:

- 1) Transacciones financieras: serán cada vez más frecuentes las consultas de clientes que desean transaccionar pagando o cobrando en cryptomonedas –la cadena de bloques es la tecnología subyacente que permite “operar en crypto.” Por otro lado, el mundo de las finanzas fue el primero en ser disruptado con *Bitcoin*, por lo que abundan casos de aplicación de *blockchain* en el mercado financiero, y muchas empresas ocupadas y preocupadas por no quedarse afuera, lo que produce una demanda de tipo *market pull* hacia abogados con formación específica en *blockchain*;
- 2) Seguros: la industria del seguro también será disruptada por la cadena de bloques, y ello producirá que aquéllos abogados

con contacto con el mundo del seguro deban estar familiarizados con esta tecnología y sus aplicaciones;

3) Sociedades: el Estado de Delaware de EE. UU desde el año 2017 permite registrar en *blockchain* a los accionistas, sus tenencias y actos societarios. El dato es relevante, ya que 2/3 de las empresas Fortune 500 de EE.UU están constituidas en dicho estado;

4) Títulos de propiedad y tracto sucesivo: cada vez será más frecuente ver registros dominiales que migran a la cadena de bloques, destacándose el caso de Dubai que ya ha migrado todo

su registro inmobiliario a la *blockchain* ^[8], tendencia ésta que se augura global, con lo cual los abogados tomarán contacto con la tecnología subyacente sobre la que se migran los registros, con especial énfasis e impacto en el principio del tracto sucesivo registral ^[9] .;

5) Autenticación e identidad: en poco tiempo, la autenticidad de origen de determinados productos, o la identidad de personas o entidades podrá ser acreditada mediante sistemas que corren en una cadena de bloques. Como se verá en este Manual, existen ya muchas empresas que ofrecen servicios notariales en *blockchain*, para acreditar la existencia y autoría de documentos, su fecha de creación y si ha sido modificado;

6) Custodia de documentos: la digitalización de documentos ya permite su almacenamiento remoto, y la *blockchain* permitirá su custodia de modo seguro y accesible bajo ciertas condiciones por partes interesadas; los abogados deberán entender la lógica de estos depósitos documentales para poder extraer de ellos la información que requieran para mejor servir a sus clientes;

7) Propiedad intelectual: la industria de la música, el cine y la edición comienzan a utilizar la cadena de bloques en distintos ámbitos de sus líneas de negocio, con foco por ahora en la distribución digital;

8) Contratos inteligentes: el objeto de estudio de este Manual, sin dudas, será fértil campo para la innovación y el

emprendedorismo. Quienes innoven y emprendan en esta materia requerirán del consejo legal adecuado y eficiente para el diseño de propuestas de valor sustentables, incluyendo, en ocasiones, la mediación en conflictos generados por la utilización de *Smart Contracts*, el trabajo multidisciplinario con desarrolladores y programadores, la revisión legal de los contratos por los cuales se contrata la programación de *Smart Contracts*, la estandarización de términos en *Smart Contracts* ^[10], y, en general, asesorar sobre el cumplimiento (o incumplimiento) de normas y regulaciones que rijan determinadas materias; y

9) Finalmente, siendo normalmente los abogados asesores legales clave de funcionarios públicos encargados de dictar y aplicar leyes y reglamentaciones, un conocimiento acabado de la *blockchain* les permitirá asesorar de mejor forma en el diseño y aplicación de leyes y de sus reglamentaciones y resoluciones, las que, se adelanta, comenzarán sin dudas a proliferar a un ritmo cada vez más acelerado.

Pero existen aún más razones para justipreciar el inmenso impacto que la cadena de bloques tendrá en el mundo del Derecho.

En efecto, con un marcado enfoque de *technology push* muy parecido al que masificó el uso de Internet a finales del Siglo XX, *blockchain* permite también pensar en nuevas formas de resolver conflictos en el mundo digital. En este sentido, el caso de la firma Kleros ^[11] es sin dudas muy prometedor. Su fundador, emulando las prácticas de resolución de conflicto existentes en Grecia, desarrolló un interesante protocolo en *blockchain* que sirve para resolver disputas on line, conflictos que representan entre un 3% y un 5% del total de las transacciones on line ^[12].

En efecto, la visión de Kleros es construir una red descentralizada de jurados para adjudicar disputas en diferentes industrias, con un ojo puesto en la adopción masiva de contratos inteligentes ^[13], lo que requerirá sin dudas

de la implementación de un mecanismo de “escotilla de escape”, ya que los contratos inteligentes, antes que un contrato, son software, y como tal –y como se verá en varios puntos de este Manual–, el software no es *error-free*. Kleros ofrece esa necesaria escotilla de escape descentralizada, un método de corrección de errores para revocar contratos inteligentes cuando el cumplimiento se ha vuelto irrazonable. Una escotilla de escape que funciona sin reintroducir arbitrariedad y corrupción en el sistema. Esto permitirá extender el uso de contratos inteligentes a un número creciente de industrias [\[14\]](#).

Ahora bien, a lo largo de este Manual se verán muchas formas de impacto de la *blockchain* en el Derecho, pero debe tenerse en cuenta que el impacto será también a la inversa.

Es falsa (o al menos ingenua) la creencia que sostiene que la *blockchain*, sus plataformas y protocolos y sus funcionalidades pueden operar completamente “al margen de la Ley” [\[15\]](#). A medida que que la tecnología de la cadena de bloques permea en sectores que abracen sus ventajas y funcionalidades, los sistemas legales de todo el mundo (y los abogados y jueces que en ellos operan) deberán, en un momento u otro, identificar, evaluar y definir cómo resolver los conflictos que se susciten entre los que operan dentro de la red, y fuera de ella [\[16\]](#).

El desafío es encontrar un justo equilibrio entre, por un lado, esta tecnología de enorme potencial y, por el otro, el sistema legal y social donde se inserta, resguardando *pari passu* las garantías constitucionales de ejercer industria con fines lícitos, asociarse, innovar y emprender, y, por el otro, la paz social. Para ello, la relación entre Derecho y *blockchain* debe ser colaborativa y de diálogo asertivo, lo que requiere que abogados y programadores hablen un mismo idioma.

Justamente, a tratar de explicitar el idioma (o nivelar el lenguaje) para que ese diálogo pueda existir, es que se dedica este Manual, bajo la firme convicción que la *blockchain* es una *Tecnología Fundamental* como lo fue Internet, y que el mejor resultado posible se obtendrá de desarrollos híbridos donde el Derecho y la *blockchain* se encuentren a mitad de camino y no se

niegen mutuamente ^[17].

Otra razón –y quizás, la más importante– por la cual este Manual se escribe pensando –principalmente– en los estudiantes de Derecho, es que luego de 15 años de docencia universitaria en grado y posgrado en Escuelas y Facultades de Derecho de cinco Universidades, públicas y privadas, estoy absolutamente convencido que la educación legal actual no está a la altura de las habilidades y competencias que se demandarán al Abogado del Siglo XXI. Y no estoy solo en este pensar ^[18].

Es innegable que la formación de grado en Derecho no acentúa la innovación, ni la agilidad ^[19]. Tampoco es común que se *mezclen* contenidos legales y tecnológicos en los trayectos formativos.

Pues bien, los signos de los tiempos indican que deben vincularse intrínseca y funcionalmente los trayectos formativos del Derecho y las Ciencias de la Computación muy rápidamente, ya que en poco tiempo la industria legal será uno de los sectores más impactados por las nuevas tecnologías. La disrupción del sector legal vendrá de la mano del *Legal Tech*, combinado innovaciones inter-tecnológicas con el *Machine Learning*, la *Legal Automation*, el *Bid Data* aplicado, la *Blockchain* y los *Smart Contracts*.

Esta combinación de tecnologías producirá impactos cada vez más frecuentes y más intensos, que afectarán lenta pero persistentemente la forma de ejercer la profesión de Abogado en el Siglo XXI ^[20], profesión que deberá conocer y manejar nuevos conceptos y disciplinas tales como la *Lex Cryptographia* ^[21] acuñada por Wright y De Filippi, o el *Legal Programming* acuñado por Koulu ^[22], y utilizar cada vez más la visualización contractual mediante el *Legal Design* que impulsa la Universidad de Stanford desde su *Legal Design Lab* ^[23].

No tengo dudas que los abogados y los jueces por igual deberán prepararse para una ola imparable de lo que denomino *Incremental On-Chain Innovations*, **Io-cl**, innovaciones intra-tecnológicas que ocurrirán en el

entorno blockchain. El primer mercado disruptado con *Io-cI* fue el mercado financiero con el surgimiento de Bitcoin, que será nuevamente disruptado con el inminente lanzamiento masivo del *Yuan Digital*, una Central Bank Digital Currency que será la nueva moneda China y que ya comienza a utilizarse en mayo de 2020 para el pago ciertos salarios públicos ^[24]. No tengo dudas que el segundo gran mercado en ser disruptado será el de los servicios legales y la administración de Justicia. Así, el surgimiento de las Limited Liability Autonomous Organizations (LLAOs) disruptará el derecho societario y creará las bases para un Gobierno Corporativo 2.0.

I. Blockchain: FAQs

1.1. *Blockchain*

1.1.1. *Cypherpunks*

Para comenzar a adentrarse en el mundo de la *blockchain*, es necesario previamente entender conceptos esenciales de criptografía. En relación a la transmisión de datos vía Internet, la criptografía es el conjunto de técnicas – i.e. métodos de encriptación– que protege comunicaciones frente a la presencia potencial de terceros observadores, sean éstos gobiernos, empresas o personas ^[25]. Tales métodos de encriptación permiten mantener tanto la confidencialidad de la comunicación como demostrar su autenticidad ^[26]. El nivel más básico de encriptado *on line* implica el uso de llaves públicas y privadas ^[27].

Muy asociado al deseo de proteger las comunicaciones en el ámbito digital, se encuentra la desconfianza hacia terceros que puedan interferirlas, principalmente los gobiernos. Así, a principios de 1990, se ve surgir, apalancado en Internet, a un movimiento con un fuerte tinte político libertario, conocido como los *Cypherpunks* ^[28], cuya bandera era (y es) defender la privacidad de las personas a través de la criptografía, utilizando el anonimato, firmas digitales y dinero electrónico. Proponían establecer un freno a la cibervigilancia estatal, ante la creencia que:

“We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak (...) **We must defend our own privacy if we expect to have any.** We must come together and create systems which allow anonymous transactions to take

place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.”^[29] (El resaltado es mío).

Es importante recordar la bandera de este movimiento, para vincularla con la aparición del Bitcoin veinte años después. Las criptomonedas, a diferencia de las monedas de curso legal o *fiat currency*, promueven en alguna medida la separación entre el individuo y el Estado^[30]. En efecto, era reconocido que una comunidad se define por la cooperación de sus miembros, y una cooperación eficiente requiere un medio de intercambio (dinero) y una forma de hacer cumplir los contratos, servicios éstos generalmente ofrecidos por los gobiernos^[31].

Desde 1983 se registran propuestas de creación de dinero digital configuradas con un servidor central para responder o solucionar el problema del doble gasto^[32]. Con los avances posteriores en técnicas de encriptación, cambió el enfoque para resolver el problema del doble gasto, y se presentó una importante iniciativa que se llamó *B-Money*^[33]: una forma de dinero electrónico controlada por técnicas de encriptación y no por bancos centrales o bancos comerciales, utilizando la pseudonimia a través de llaves públicas para enviar mensajes entre los miembros de la comunidad. Cada participante mantendría una base de datos separada, con la información de cuánto dinero correspondía a cada pseudónimo (i.e., a cada llave pública), de modo de evitar el doble gasto. Se podría generar nuevo *B-Money* sólo solucionando problemas matemáticos no resueltos antes. Como se verá más adelante, esta lógica es muy similar a la lógica subyacente de Bitcoin.

1.1.2. *El avance tecnológico y la Riqueza de las Redes*

Es innegable que la tecnología avanza a un ritmo muy rápido: sólo hace 40

años que el primer protocolo de Internet (TCP/IP^[34]) fue presentado en una conferencia internacional sobre comunicaciones, y hace sólo 30 años que Internet está disponible para el público en general^[35]. En 1993 el National Center for Supercomputing Applications dio a conocer Mosaic, el primer navegador gráfico de Internet; en 1995 Netscape salió a la bolsa, con una valuación de tres billones de Dólares, y allí empezó la Economía de Internet^[36]. En 1996, Johny Perry Barlow publicó la Declaración de Independencia del Cyberespacio^[37] y en 2001 la Justicia norteamericana obligó a Napster a cerrar por violación del derecho de autor^[38]. En 1998, Microsoft fue demandada por el gobierno norteamericano, por ventas atadas, una infracción *antitrust*. La demanda fue tranzada en 2001^[39].

Este primer ciclo de Internet demoró casi 40 años, pasando por las etapas de uso individual, uso local, sustitución y transformación de industrias^[40].

Pero hace sólo 12 años atrás, en Octubre de 2008, apareció *blockchain* como tecnología subyacente de Bitcoin, y ya existe un amplio consenso que afirma que se trata de una nueva *Tecnología Fundamental*^[41], igual que lo fue Internet en la década del noventa.

En sí, *blockchain* es la evolución de la economía *peer-to-peer*^[42], a la que combina con algoritmos criptográficos, bases de datos distribuidas, y mecanismos descentralizados de consenso, facilitando que las personas que la utilizan puedan acordar sobre la existencia de determinadas transacciones, y registrar su existencia de un modo seguro y auditable^[43]. No hay en ella una innovación exponencial, sino más bien incremental^[44], ya que el encriptado asimétrico de llave pública y privada es una tecnología que existe desde 1970; también existen desde 1970 las redes *peer-to-peer* que se popularizaron en la década del 2000; los mecanismos de consenso existen desde 1990, y las bases de datos distribuidas existen desde 2005^[45]. Ahora bien, cuando todos estos elementos se conjungen entre sí, emerge la *blockchain* como una forma

eficiente y novedosa de resolver el *Problema de los Generales Bizantinos* ^[46]. Y esto sí termina por abrir la puerta a una cantidad exponencial de aplicaciones de esta nueva tecnología emergente.

Se ha sostenido, con razón, que Internet está entrando en una fase de *decentralización*, entendida ésta como las (nuevas) condiciones bajo las cuales las acciones de muchos agentes se cohesionan y son efectivas, sin que exista necesidad de un reducido número de agentes que dirijan las acciones hacia un resultado efectivo ^[47]; fase opuesta a la *centralización*, entendida como un modo particular de respuesta al problema de cómo hacer que las conductas individuales de muchos agentes se cohesionen siguiendo un determinado patrón (central).

El auge de las redes descentralizadas de computadoras, combinado con nuevas formas de encriptación, da lugar a la *blockchain*, una base de datos descentralizada, distribuida, compartida, encriptada, que sirve de registro público de información, inmutable e incorruptible, lo que a su turno permite que personas que no se conocen puedan acordar sobre la existencia de determinadas transacciones, sin tener que recurrir a una autoridad central que atestigue lo ocurrido ^[48].

Hay quienes piensan que la *decentralización* que la *blockchain* ahora permite, quitará poder a las autoridades y entes centrales en el mundo de los negocios, de las comunicaciones, e incluso en la arena política, al permitir que las comunidades se organicen de manera más fluida y promoviendo la participación directa en la toma de decisiones ^[49]. Otros, más extremos en su pensamiento, ven la resurrección de un movimiento *Cypherpunk 2.0*, e incluso un ámbito fértil para la actividad delictiva, esquemas defraudatorios al estilo Ponzi, y un camino de ida hacia la anarquía y el autoritarismo ^[50].

1.1.3. *From Internet of Information to Internet of Value y a la criptoeconomía*

Muchos afirman que la *blockchain* permitirá evolucionar de una Internet de la Información hacia una *Internet del Valor* ^[51], al permitir transferir valor de una persona a otra vía Internet. *Valor*, en contexto de *blockchain*, puede significar muchas cosas: dinero, acciones, títulos de propiedad, regalías digitales, incluso un voto en una elección. Así como el *e-mail* permitió la mensajería bilateral, Bitcoin permite realizar transacciones de manera bilateral ^[52]. Así como el TCP/IP redujo drásticamente el costo de las comunicaciones, *blockchain* podría reducir el costo de las transacciones ^[53].

De la mano del avance de la encriptación, se gesta a su amparo la llamada *Criptoeconomía*, definida como un sistema económico que no está definido por límites geográficos, políticos o legales, sino por el uso de técnicas criptográficas para limitar conductas, en lugar de recurrir a terceros de confianza ^[54]. Se trata de una disciplina que estudia los protocolos que gobiernan la producción, distribución y el consumo de bienes y servicios en una economía digital y descentralizada, analizando los diseños y características de dichos protocolos ^[55].

Ahora bien, investigadores de la Universidad de Harvard creen que pueden faltar décadas para que *blockchain* pueda realizar todo su potencial, y que la rapidez de la adopción (masiva) de sus distintas aplicaciones dependerá de dos dimensiones: la novedad de cada aplicación, por un lado, y, por el otro, la complejidad y coordinación que demanda cada nueva aplicación ^[56].

Se afirma que esta tecnología fundacional deberá pasar por cuatro estadios o fases secuenciales –uso individual, uso local, sustitución y transformación–, que se ilustran en la Tabla ^[57] más abajo:

Alta	(3) Sustitución Gift cards en Bitcoin	(4) Transformación <i>Smart Contracts</i>
------	---	---

C O M P L E J I D A D Baja		
	(1) Uso individual Pagos con Bitcoin (Pizza Day!)	(2) Uso local <i>Blockchains</i> permitidas para procesamiento de transacciones financieras
	NOVEDAD	

Alta

1.1.3.1. La pizza más cara de la historia

El 22 de Mayo de 2010 tuvo lugar la primera compra de un bien físico pagado con Bitcoin, la primera transacción con “el mundo real” en la historia de *blockchain*. Una persona del Estado de Florida, llamada Laszlo Hanyecz ofreció en un foro sobre Bitcoin comprar dos pizzas a condición que fueran entregadas en su casa, pagando en Bitcoin. En el foro habría un hombre de Inglaterra, que aceptó la oferta, le compró dos pizzas a Laszlo en Papa John’s, y recibió en pago 10.000 bitcoins [\[58\]](#).

1.1.4. Antes de Bitcoin: BitGold

Si bien Bitcoin fue la primera aplicación exitosa de la *blockchain*, no fue la primera vez que se pensó en una solución de dinero digital. Además de *B-Money*, debe resaltarse el caso de BitGold. Nick Szabo [\[59\]](#) es, sin dudas, un

forward-thinker. Es quizás el creador del concepto de *Smart Contract*, hace nada más y nada menos que casi 30 años ^[60]. Y también desarrolló un concepto de moneda digital, al que llamó BitGold ^[61]:

"Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function.". The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards." (el resaltado es mío).

BitGold fue un precursor de Bitcoin, y de hecho, muchos creen que Nick

Szabo es en realidad Satoshi Nakamoto ^[62].

1.1.5. Reeditando viejas discusiones (de cuando irrumpió Internet)

En el año 1999, Lawrence Lessig, un Profesor de Contratos y Propiedad Intelectual, publicó un libro llamado *Code and other Laws of Cyberspace*, en el que en algún modo le contestaba a Johny Perry Barlow relativizando su Declaración de Independencia del Cyberespacio del año 1996. Obicamemente, se generó un gran debate sobre la regulación de Internet ^[63].

Dos bandos se formaron: los ciberlibertarios, por un lado, que sostenían que la naturaleza distribuida y global de Internet la volvían ingobernable por los Estados, colocándola fuera del alcance de la Ley, debido principalmente al anonimato que Internet permite y a la gran movilidad de los participantes en el ciberespacio, pudiendo “relocalizarse” libremente dentro del ciberespacio ^[64]. Por otro lado, emergieron los ciberpaternalistas, sosteniendo que nada intrínseco a la naturaleza de Internet la eximía de cumplir las Leyes. Entre éstos se inscribió Lessig, quien sostenía que las leyes ordinarias que rigen las conductas en el mundo real regulaban también la conducta en el ciberespacio, aunque la eficacia de este control dependía de las características del ciberespacio, pudiendo los Estados regular el código –i.e. programación– en sí, y a los programadores que programan el contorno del ciberespacio.

El tiempo le dio la razón a los ciberpaternalistas ^[65], pero la pregunta que la Internet del Valor hace (nuevamente) surgir, es si los Estados podrán (o deberán) controlar su desarrollo y expansión, del mismo modo en que lo hicieron con la Internet de la Información. En 2015, Lessig ^[66], un convencido de que la *blockchain* es la mayor innovación desde la invención de Internet y que beneficiará, sobre todo, a los más pobres y vulnerables, afirmó que el potencial de la *blockchain* no se limita a sus aspectos (atributos) tecnológicos, sino que también permeará (y mucho) en el ámbito político y

gubernamental, en un mundo sediento de transparencia frente a la oscuridad de la corrupción global. Sin embargo, Lessig afirma que las viejas discusiones en torno al ciberespacio serán reeditadas producto de la *blockchain*, y que nuevamente aparecerán pensamientos libertarios extremistas, que no son más que una falacia. Por el contrario, Lessig afirma, a secas, que la *blockchain* y su ecosistema necesitará a las Leyes y a los Estados (regulaciones), para hacer cumplir contratos “implícitos” y cláusulas no explícitas (i.e., no programadas), y para gestionar también eventuales contingencias que se produzcan por eventos previsible pero inevitables, incluso en un mundo plagado de *Smart Contracts* ^[67]. En sus palabras, “code needs law”.

1.1.6. *Blockchain vs. DLTs vs. Sistemas Distribuidos*

Es importante diferenciar técnicamente la *blockchain*, de las *distributed ledger technologies* (DLTs), y de los sistemas distribuidos. Los sistemas distribuidos son aquellos en los que sus componentes (hardware y/o software) están distribuidos en computadoras en red, las que se comunican y coordinan acciones solo mediante el envío de mensajes ^[68]. PayPal, el GPS, y Google, son todos ejemplos de sistemas distribuidos.

Dentro del género (amplio) de sistemas distribuidos, se pueden inscribir tanto las DLTs, por una parte, como la *blockchain*, por la otra ^[69], pero existen diferencias entre ambas, ya que hay una relación de género a especie entre las DLTs y la *blockchain*.

Desde un punto de vista técnico, una DLT es simplemente una base de datos que gestionan varios participantes y no está centralizada. No existe una autoridad central que ejerza de árbitro y verificador. El registro distribuido aumenta la transparencia -dificultando cualquier tipo de fraude o manipulación- y el sistema es más complicado de ‘hackear’ ^[70].

La *blockchain*, por su parte, no es otra cosa que una DLT con una serie de características particulares: (i) también es una base de datos -o registro-compartida, pero en este caso mediante (ii) bloques que, como indica su propio nombre, forman una cadena, y los bloques se cierran con una especie

de (iii) firma criptográfica llamada ‘*hash*’; el siguiente bloque se abre con ese ‘*hash*’, a modo de sello lacrado. De esta forma, se certifica que la información, encriptada, no se ha manipulado ni se puede manipular ^[71].

1.1.7. Algunas definiciones (y un ejemplo clásico para ilustrar su funcionamiento)

A continuación se señalan distintas definiciones dadas por autorizados doctrinarios, no sin antes advertir al lector que la palabra *blockchain* puede ser indistintamente utilizada para designar (i) el género de las tecnologías de cadena de bloque, (ii) una especie del género, aquél subconjunto de *blockchains* públicas dentro del ecosistema *blockchain*, o (iii) una subespecie del género, i.e. la cadena de bloques subyacente a la criptomoneda *bitcoin* ^[72].

GARTNER, en una obra reciente ^[73], define a la *blockchain* como un mecanismo digital para crear un libro de registros digital y distribuido, en el cual dos o más participantes integrantes de una red *peer-to-peer* pueden intercambiar información y activos de manera directa, sin intermediarios. La *blockchain* autentica a los participantes, valida que éstos tengan los activos sobre los que quieren tranzar, y registra los intercambios en dicho libro de registros digital, del cual todos los partícipes tienen una copia actualizada y cuyos asientos o registros, que no son modificables, son cronológicamente organizados y empaquetados en bloques, encriptados, y vinculados unos a otros. Sus elementos esenciales son:

- i) distribución: los participantes están físicamente separados, pero conectados a través de una red de la cual son nodos, con acceso al registro;
- ii) encriptación asimétrica y pseudonimia;
- iii) inmutabilidad, salvo que se acuerde lo contrario;
- iv) tokenización: las transacciones en una *blockchain* involucran la transferencia segura de valor, en forma de *tokens*, que es la representación digital de algún activo, o una forma de retribuir a los participantes, o incluso datos agrupados; y

v) descentralización: la red y sus protocolos son operados y están mantenidos en múltiples computadoras de la red distribuida, lo que significa que no hay una sola computadora que corra la *blockchain*.

Cuando una *blockchain* reúne estos cinco elementos, su valor se maximiza [74]. Wright y De Filippi la definen como una base de datos de transacciones cronológica, administrada por una red de computadoras, donde la cadena de bloques está encriptada y organizada en conjuntos de datos más pequeños, llamados bloques. Cada bloque contiene información sobre una determinada cantidad de transacciones, junto con una referencia –llamada *hash*– al bloque inmediato precedente, junto con la solución a un complejo problema matemático que se utiliza para validar los datos asociados a ese bloque en particular. Una copia de toda la cadena está alojada en cada computadora de la red –llamadas nodos–, y se sincroniza –actualiza– periódicamente de modo que todas las computadoras alojen la misma base de datos [75]. Toda operación en una *blockchain* es validada a través de una huella digital, creada a través de una función de *hashing*, e.g., SHA256 en el caso de Bitcoin [76]. Para garantizar que solo transacciones legítimas se agregan a la cadena, la red de computadoras debe confirmar que la nueva transacción es válida y que no invalida ninguna transacción precedente, de modo tal que sólo se agregará un nuevo bloque a la cadena si existe un consenso en tal sentido entre los nodos. Este consenso entre las computadoras de la red se puede obtener a través de distintos mecanismos de voto, siendo el más común el de *Proof Of Work* (PoW) [77], que depende a su vez de la cantidad de poder de cómputo donado para mantener la red. Una vez que un bloque nuevo se agrega, no puede ser borrado, y las transacciones en él contenidas pueden ser verificadas por toda la red.

Por su indudable influencia en el mundo de la *blockchain*, a continuación se transcribe la definición que Vitalik Buterin ha dado:

“Public *blockchains*: a public *blockchain* is a *blockchain* that **anyone** in the world **can read**, anyone in the world can **send**

transactions to and expect to see them included if they are valid, and anyone in the world can **participate** in the consensus process –the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public *blockchains* are **secured by crypto economics** – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These *blockchains* are generally considered to be ‘fully decentralized’^[78]. (el resaltado es mío)

También es útil traer a colación otra definición de Vitalik Buterin, en términos menos técnicos, quien define la *blockchain* como “una computadora mágica a la cual cualquiera puede subir programas y dejarlos que se autoejecuten, siendo visible para todos el historial pasado y el estado presente de cada uno de esos programas y que cuenta con una garantía muy fuerte, criptoeconómicamente reforzada, que asegura que los programas se ejecutarán exactamente en el modo previsto en el protocolo de la *blockchain*”^[79].

Eliza Mik la define como un libro encriptado, descentralizado y validado entre pares, que muestra un registro público, cronológico y permanente de todas las transacciones previas, similar a una plantilla de cálculo de Excel en la que cualquiera puede agregar filas, pero nadie puede borrar o modificar los datos cargados. En su origen, fue diseñada para un solo fin: evitar el “doble gasto” de bitcoins en un sistema que no cuenta con una autoridad central que controle la emisión o la transferencia de bitcoins. El problema del doble gasto fue resuelto visibilizando para todo el mundo todas las transacciones, pasadas y presentes, de bitcoins^[80].

Karen Yeung^[81], por su parte, la define como una base de datos distribuida, en la que sólo se pueden anexar datos (*append-only*), que es

colaborativamente almacenada, mantenida y actualizada por una red de computadoras, cada una de las cuales tiene una copia idéntica de dicha base de datos. Métodos criptográficos permiten consensos matemáticos para confirmar la consistencia del registro digital de cada transacción, y dicho registro es inmutable, no pudiendo ser borrado o alterado en condiciones normales ^[82]. La información en una *blockchain* se representa por *tokens* criptográficos, agrupados en bloques, que garantizan técnicamente la autenticidad de la información que contienen. Las *blockchains* registran la alocación de estos tokens en cuentas anónimas, y automáticamente registran todos los intercambios de estos *tokens* entre cuentas, actualizando automáticamente la última copia de la cadena. La seguridad y precisión de esta base de datos se mantiene mediante técnicas computacionales en las que “llaves criptográficas” y firmas digitales permiten controlar quién puede hacer qué en el base de datos compartida.

Werbach ^[83] conceptualiza la *blockchain* como un libro de registros distribuido, pero demostrablemente correcto, del cual cualquiera puede mantener una copia que se actualiza dinámicamente de manera simultánea, sin que exista un administrador central. Esto permite, por un lado, que se pueda confiar en las transacciones registradas, sin tener que confiar en instituciones, gobiernos o intermediarios, y, por el otro, al haber un solo registro distribuido, no es necesario que existan múltiples registros individuales, con lo cual es innecesario realizar conciliaciones y ello reduce los costos de transacción. Este nuevo “paradigma” es seguro gracias a la criptografía y a la implementación en la red distribuida de un mecanismo de consenso, que permite confiar en la información que el sistema arroja, sin tener que confiar en ningún actor dentro del sistema.

Raskin ^[84] define la *blockchain* como bases de datos creadas en una red sin ninguna autoridad central, mantenidas por cada computadora de la red que use el software. Son conjuntos de datos verificados por los miembros de una red *peer-to-peer*. La unidad de una *blockchain* es un bloque, que contiene determinada información. Cada bloque es verificado por un gran número de computadoras de la red, los nodos, y luego se anexa al último bloque verificado.

Jared Arcari^[85], por su parte, señala que distintos términos compiten para explicar la mecánica de la *blockchain*, incluyendo *distributed ledger technology*, *shared ledger technology*, y *mutual distributed ledger*, y también por las funcionalidades o accesos que cada *blockchain* otorga a cada usuario, que van desde accesos que sólo permiten leer, que permiten escribir, o que permiten leer y escribir. La tecnología de la *blockchain* está diseñada para evitar el problema del “doble gasto”, y en el caso de la *blockchain* de Bitcoin, esto se logra *hasheando* las piezas de información, y agrupándolas en bloques de información *hasheada*, utilizando estampas de tiempo, y que se agregan a la cadena sólo si los miembros de la red lo confirman a través de la PoW. La cadena sirve entonces como un registro continuo de todas las transacciones previas hechas por sus usuarios, evitando “la duplicación”, y manteniendo el registro histórico^[86].

Fulmer^[87], a su turno, define la *blockchain* a través de sus características esenciales: descentralización, mecanismo de consenso de la Prueba de Trabajo (PoW, en inglés) e inmutabilidad. Al combinarse estos tres elementos, es posible realizar transacciones digitales sin tener que recurrir a un intermediario de confianza que las atestigüe, recurriendo en cambio a una red de usuarios que mantienen y monitorean el registro distribuido. Este registro es transmitido a toda una red de computadoras, no existiendo un único depositario central. Para que el registro sólo incorpore transacciones legítimas, la red incentiva a ciertos usuarios para que verifiquen cada transacción antes de ser ingresadas al registro. Una vez verificada una transacción, se la agrega a un bloque, que está criptográficamente vinculado al bloque anterior, y así sucesivamente. Al estar todos los bloques vinculados –*hasheados*– con su predecesor, es prácticamente imposible modificar o falsificar información precedente.

Nick Szabo afirma que la *blockchain* es una computadora virtual, en la nube, compartida entre muchas computadoras tradicionales y protegida por criptografía y tecnologías de consenso^[88]. Por su propio diseño, cada computadora verifica el trabajo de la otra, utilizando un mecanismo de consenso probabilístico y anonimidad. Es un registro único donde se almacenan transacciones en bloques a medida que ocurren, permitiendo a las

partes acceso en tiempo real a la información, generando un código de programación que permite una “confianza reducida”, ya que permite confiar en él en lugar de confiar en el dueño de la computadora. Esta tecnología ofrece un nivel de seguridad muy superior comparado a la tecnología de los servidores de Internet centrales. Las técnicas criptográficas empleadas en la *blockchain* proveen evidencias perennes sobre todas las transacciones y demás información asociada subida a la cadena, de un modo muy superior a la seguridad de otros sistemas distribuidos o peer-to-peer. Ahora bien, señalaba Szabo en 2014 que esta tecnología, on line y distribuida, es mucho más lenta y costosa que la tradicional ofrecida por servidores web centrales, unas 10.000 veces más lenta, o sea que es como usar un programa informático en el año 1985 ^[89].

Por su claridad y precisión, se transcribe a continuación la definición que dan Kaal y Calcaterra:

“A *blockchain* is a shared digital ledger or database that maintains a continuously growing list of transactions among participating parties regarding digital assets – together described as “blocks.” The linear and chronological order of transactions in a chain will be extended with another **transaction link** that is added to the block once such additional transactions are validated, verified and completed. Cryptographic hashes increase *blockchain* security. **Cryptographic hashes** are complex algorithms that use details of the existing entirety of transactions of the existing *blockchain* **before the next block is added** to generate a unique hash value. That hash value **ensures the authenticity of each transaction before it is added** to the block. The smallest change to the *blockchain*, even a single digit/value, results in a different hash value. The chain of transactions is distributed to a limitless number of participants, so called nodes, around the world in a public or private peer-to-peer network. Network connectivity allows multiple copies of the *blockchain* to be available to all participants across the distributed network. **The decentralized**

fully distributed nature of the *blockchain* makes it practically impossible to reverse, alter, or erase information in the *blockchain*. *Blockchain*'s distributed consensus model allows **node verification of transactions without comprising the privacy of the parties.** Therefore, *blockchain* transactions are arguably safer than traditional transactions that require a third-party intermediary validation of the transactions.” [\[90\]](#) (el resaltado es mío).

Es interesante la definición que brindan el BANCO INTERAMERICANO DE DESARROLLO y el FORO ECONÓMICO MUNDIAL: un libro compartido y distribuido de registros o transacciones, abierto a inspección para cada participante de una red [\[91\]](#).

El Parlamento Europeo, por su parte [\[92\]](#), remarca que las *blockchains* ofrecen una funcionalidad de registro de transacciones, sin una arquitectura centralizada, sino distribuida, de modo que cada partícipe tiene una copia del registro actualizado. Para incluir nuevas transacciones, se utilizan técnicas para validar que la transacción es posible y es correcta, y se forman paquetes de transacciones llamados bloques, que se van agregando cronológicamente formando una cadena.

Finalmente, Thibault Schrepel [\[93\]](#), Profesor asociado en Harvard University y creador de la ESCUELA DE *BLOCKCHAIN* de la Universidad de Utrecht en los Países Bajos –a donde el autor inició sus primeros pasos en esta tecnología–, conceptualiza la *blockchain* como un registro abierto y distribuido, que registra todo tipo de transacciones entre sus usuarios. Estas transacciones, una vez registradas en la cadena, no pueden ser generalmente modificadas [\[94\]](#) y, en principio, pueden ser vistas por todos los usuarios de la red sin restricción. Por ese mismo carácter inmutable, la *blockchain* recurre a distintos mecanismos de consenso para asegurar que la información y las transacciones que la representan sean fidedignas, por lo que se construye una confianza *en la red* ya que no acceden a ella datos no validados previamente. Las *blockchains* pueden modularse en su arquitectura para que los usuarios

tengan distintos permisos, i.e., leer la información, proponer nueva información y escribir –validar– información. Señala Schrepel que en las *blockchains* públicas, es característico de ellas la existencia de pseudonimia a través de llaves públicas que se corresponden a cada nodo de la *blockchain*, y que puede dificultar saber la identidad real de la persona u organización operando el nodo.

Como se puede apreciar, abundan las definiciones, y es difícil elegir alguna. Quizás la mejor definición de *blockchain* sea una mera descripción general de su funcionamiento –al menos, de las *blockchains* públicas, que se estudian más abajo [\[95\]](#). La *blockchain* es, entonces:

- i) una serie de bloques de datos, cada uno de ellos conteniendo información acerca de eventos que han ocurrido recientemente. Esta información puede ser de la más variada índole, desde la compra de productos, transferencias de propiedad, registros de propiedad, o cobros de regalías por cualquier concepto. La verificación de los datos a ser agregados a la cadena es realizada por mineros, mediante procesos criptográficos que demandan gran poder de cómputo. Cada bloque de información
- ii) está *hasheado*, lo que significa que está criptográficamente vinculado al anterior y encriptado;
- iii) cada bloque contiene una referencia al bloque anterior, una lista de las transacciones incluidas en él, una estampa temporal, y una prueba criptográfica que garantiza la veracidad de la información.
- iv) Los bloques se transmiten a todas las computadoras de la red, y los nodos de la red verifican –por mayoría o por algún otro procedimiento pre-pactado– la validez de cada bloque, antes de incorporarlo a la cadena de la cual no podrán ser removidos. Pero, ¿cómo funciona?

Si uno tiene en cuenta que esta tecnología es una forma posible de resolver el problema del *doble gasto* –es decir, es una tecnología anti-fraude– recurriendo a la criptografía asimétrica, o de llaves públicas y llaves privadas

que están vinculadas entre sí ^[96], es relativamente fácil entender cómo funciona. Veamos. Cada agente de la cadena de bloques tiene (i) una llave privada y desconocida salvo para su dueño (que debe ser resguardada como cualquier contraseña de un *home banking* actual) y (ii) una llave pública, que todos los agentes de la cadena pueden ver. Una transacción se inicia cuando el *futuro* dueño de un *token* (e.g., una moneda digital, cualquier activo digital) envía su llave pública al *actual* dueño del *token*, quien puede inmediatamente transferirle la moneda digital –u otro activo *on-chain*– al insertar su llave privada, que opera como una firma digital *hasheada* ^[97]. Las llaves públicas de todos los participantes son direcciones generadas mediante criptografía, que están almacenadas en la *blockchain* y todo el mundo puede ver. Toda moneda digital está asociada a una llave pública, siempre, y una transacción en la criptoconomía es simplemente la transferencia entre llaves públicas –i.e., cuasi-direcciones *on line*– de algún *token*. La particularidad muy sobresaliente de este esquema es que las llaves públicas no están vinculadas a la identidad real de una persona u organización. Si bien todas las transacciones son trazables, porque quedan registradas las transferencias entre llaves públicas, no se puede saber a quién corresponde la llave pública, a no ser que se acceda a esta información. A continuación, ejemplos de llaves públicas y privadas ^[98]:

Imagen 2: llave pública

```
>>> print(wallet1.sec)
b'036cbcd6c13b0d75c04500ece0047e7901d54b588e29620a802c29841314c1f01c'
```

Public Key shown as hexadecimal representation of bytes

Imagen 3: llave privada


```
>>> print(pk.secret)
5347189351573579406671668254969061247288098698306548937424096207815889665932
```

Generated Private Key

Kaal y Calcaterra [\[99\]](#) señalan que lo que ha vuelto tan exitosa a la arquitectura de la *blockchain*, es su habilidad de resolver problemas aparentemente contradictorios:

- 1) Es una base de datos que le da anonimidad a sus usuarios: dentro de la cadena de bloques, existen llaves públicas que no están vinculadas a la identidad real del dueño de la dirección;
- 2) A la vez, toda la lista de transacciones está disponible y es pública, y cualquier persona con Internet puede ver todo el historial de transacciones que corresponde a cada llave pública, lo que a la vez garantiza la *confidencialidad* pero permite *confiar* en la precisión y corrección del registro;
- 3) Al ser un sistema abierto, cualquier persona con Internet puede participar editando una parte de la cadena de bloques, y a la vez es un sistema muy seguro por no encontrarse toda la información centralizada en un único servidor físico; y
- 4) El sistema es autónomo, en el sentido de que no depende de una autoridad central que mantenga su integridad, y a la vez un sistema abierto de protocolos de consenso regula la forma en que se agregan nuevos bloques a la cadena y cómo se la mantiene. A su vez, se están desarrollando importantes avances en materia de protocolos de consenso, migrándose de PoW a PoS, como se verá más abajo [\[100\]](#).

1.1.8. Características esenciales de la blockchain

1.1.8.1. Decentralización

Como se ha afirmado más arriba, la blockchain depende de una red de

computadoras peer-to-peer que la mantenga ^[101], cada computadora de la red se denomina nodo, y cada nodo corresponde a un usuario. Cada usuario tiene (i) una llave pública, i.e. una cuenta de usuario anónima pero públicamente visible en la blockchain, (ii) una llave privada, i.e. una clave sólo conocida por cada usuario y necesaria para realizar transacciones, y (iii) un token, que puede ser una criptomoneda, e.g. Bitcoin, Ether, etc., pero también puede ser un conjunto de información de cualquier naturaleza. Decentralización implica la inexistencia de un único servidor central alojando información físicamente en único lugar; las copias de las blockchains están distribuidas en tantos nodos como cada blockchain tenga.

Por ser una red descentralizada en las computadoras que la integran, *Blockchain* permite pensar en nuevas formas de comunicación e intercambio de información *online*, sin que sea necesario que las comunicaciones y archivos deban pasar por un servidor central o una plataforma *online* (e.g., Gmail, Dropbox) ^[102]. La información puede ser publicada en el registro distribuido, encriptada, y distribuida en miles de computadoras, haciendo virtualmente imposible que una única entidad la controle. A su vez, los datos así distribuidos en cada copia de la *blockchain* alojada en cada nodo hacen muy difícil, sino imposible, que un hacker pueda alterar o modificar la información, ya que debiera modificar cada copia distribuida en cada nodo ^[103] de la red. Desde la visión del usuario, la *blockchain* emula los (hoy muy) comunes servicios de *cloud computing*, aunque técnicamente operan de un modo muy distinto ^[104].

1.1.8.2. Mecanismos de consenso

Hasta el surgimiento de blockchain, no era posible coordinar acciones individuales en Internet sin recurrir a un organismo central que atestiguará que los datos son fidedignos. Un grupo de individuos no relacionados entre sí no podían confirmar la ocurrencia de un evento sin consultar a un órgano central para verificar si una transacción era válida y no era fraudulenta ^[105]. Este problema o dificultad práctica es objeto de estudio en la ciencia de la

computación desde finales de la década de 1980, y es conocido como el problema de los Generales Bizantinos. La respuesta a este problema daría respuesta a esta pregunta: ¿Cómo hacer para que las computadoras de un sistema distribuido puedan acordar sobre un determinado hecho, sin tener que recurrir a un tercero extraño que valide información, y que per se estará siempre expuesto a ataques por parte de agentes malintencionados? [\[106\]](#)

Dicho en otros términos, la técnica del consenso permite que los miembros de una red confíen en que sus registros son correctos y consistentes, íntegros [\[107\]](#). Sin esta tecnología propia de la blockchain, cualquier miembro de la blockchain de Bitcoin podría gastar varias veces la misma bitcoin –esto se conoce como el problema del doble gasto, que será varias veces referido en este Manual–, o afirmar que tiene más bitcoins que las que realmente tiene, a lo que se suma que es relativamente fácil en sistemas digitales crear muchas cuentas o usuarios falsos, en lo que se conoce como el Sybil Attack. Estos problemas fueron resueltos por Nakamoto de manera muy inteligente, combinando nociones de encriptación y de Teoría de los Juegos [\[108\]](#).

Blockchain resuelve el problema de los Generales Bizantinos a través de un enfoque probabilístico, dado en llamar el *Consenso de Nakamoto* [\[109\]](#). La información que se transmite por la red de computadoras es verificada usando problemas matemáticos, que sólo pueden ser resueltos con gran poder de cómputo. Hipotéticamente, para que se validen informaciones *incorrectas* y se agreguen a la cadena, el atacante debiera controlar la mayoría del poder de cómputo de la red, lo que tiene una probabilidad poco alta.

En Bitcoin, la primera *blockchain* exitosamente desplegada, los nodos mineros resuelven estos complejos problemas matemáticos (i.e., PoW), y otros nodos verifican que la respuesta no se corresponda a una transacción anterior. Existen otros mecanismos de consenso que no requieren tanto poder de cómputo, como se verá seguidamente, pero la idea esencial es que *una mayoría dada de nodos deben sí o sí acordar sobre determinado hecho, para que tal información se agregue a la cadena como un bloque nuevo*. Sin acuerdo previo, no hay bloque nuevo.

La doctrina en general identifica este proceso genéricamente como

protocolos de consenso. Existen distintas formas de alcanzar el consenso, y cada una tiene consecuencias en materia de tiempo, escalabilidad y costos de agregar bloques nuevos [\[110\]](#).

1.1.8.2.1. Protocolos de consenso

Los protocolos de consenso garantizan que los datos alojados en una *blockchain* sean correctos, y que todos los nodos tengan acceso a ellos. Por lo tanto, el consenso protege la integridad y minimiza el riesgo de ataque por parte de agentes malintencionados [\[111\]](#).

En este sentido, el consenso es entendido como un proceso, por medio del cual una red de nodos *ordena* las transacciones y *valida* los bloques que las contienen *antes* de ser incorporados a la cadena. Cualquier protocolo de consenso debiera confirmar la *corrección* de todas las transacciones *propuestas* en un bloque, de acuerdo a las reglas de consenso estipuladas [\[112\]](#).

Según el tipo de *blockchain* de que se trate, los mecanismos de consenso se pueden diseñar de distintos modos, desde algoritmos del tipo de lotería como el PoET [\[113\]](#), hasta sistemas de votación como en los protocolos RBFT [\[114\]](#); lo esencial a retener aquí es que el consenso se materializa en un protocolo, que contiene instrucciones que le dicen a la *blockchain* cómo gestionar información nueva.

En la primera *blockchain* (Bitcoin), el consenso programado opera a través de incentivos y recompensas; el protocolo de consenso aprueba nuevos bloques que se incorporan, sin tener que validar esa información previamente con terceros ajenos u organismos centralizados. Existen muchos protocolos de consenso [\[115\]](#), y éstos varían a su vez según se trate de *blockchains* públicas o privadas, pero los más usados en 2020 son *Proof Of Work* (PoW) y *Proof Of Stake* (PoS).

En PoW, los nodos de la red que son mineros compiten entre sí para resolver problemas matemáticos de complejidad creciente, para lo cual deben contar con un equipamiento computacional acorde. Cada vez que se quiere agregar información a la *blockchain*, e.g., transferir un bitcoin a alguien, para

que esa transacción se agregue, debe necesariamente resolverse un nuevo problema matemático –i.e. criptográfico– muy complejo [\[116\]](#). El primer nodo que resuelve el problema lo presenta al resto de los mineros para que verifiquen la respuesta, y si el 51% o más de los demás mineros validan la respuesta dada al problema matemático, entonces se minará un nuevo bloque que se agregará a la cadena, y contendrá la información encriptada acerca de la transacción de que se trate, y el minero exitoso ganará una cantidad determinada de bitcoins –*block reward*– [\[117\]](#) y comisiones por transacción [\[118\]](#). Este método provoca que si una persona quisiera agregar información falsa a la red, debería dedicar muchos recursos para intentar agregar un bloque incorrecto, que probablemente será detectado por el resto de los mineros, salvo que el 51% de los mineros acuerden agregar información falsa [\[119\]](#).

Imagen 4: granja de mineros



La imagen [\[120\]](#) son 45.000 computadoras en Suecia, todas trabajando en la resolución de complejos problemas matemáticos, cuya resolución *per se* no importa mucho, pero cada vez que resuelven uno de ellos, sus dueños ganan bitcoins por minar bloques. También se ocupan de procesar transacciones y actualizar la *blockchain*. Evidentemente, tantas super computadoras trabajando consumen mucha energía, incluido para refrigerar los sistemas. Un estudio de 2019 estimó que toda la minería del año 2018 habría consumido 31.3 Terawatt-hora de electricidad, y generado la equivalencia de 17.3 megatonnes de dióxido de carbono [\[121\]](#). El costo de toda la red de minería de bitcoins se estimó en 700 millones de Dólares anuales, y cada transacción consume, aproximadamente, la misma energía eléctrica que un hogar durante cinco días [\[122\]](#).

En PoS, en cambio, los nodos que validan nuevos bloques no compiten en velocidad, ni tampoco tienen que resolver complejos problemas matemáticos que requieren mucho poder de cómputo, sino que el validador que más participación tenga en la *blockchain* [\[123\]](#), será el que más probabilidad tenga de ser elegido para agregar nuevos datos a la misma [\[124\]](#).

Este protocolo solo verifica la tenencia i.e. *stake* del validador, y quien más tiene, más bloques podrá agregar. Esta última particularidad del PoS ha sido criticada por Igor Artamonov, sosteniendo que el PoS favorecerá la centralización de validadores en los grandes inversores –en este caso, de Ethereum– ya que son éstos los que tienen el 70% de las monedas emitidas [\[125\]](#). En PoS, la cantidad de monedas requerida para poder validar se llama *target*, y es ajustada periódicamente por cada *blockchain* para asegurar un tiempo constante de validación [\[126\]](#). Si un validador comete o intenta cometer un fraude agregando información inexacta, perderá su *stake*, *ergo*, perderá la posibilidad futura de agregar nuevos datos a la *blockchain*. La *blockchain* Ethereum está –aparentemente– migrando desde PoW a PoS en 2020 o 2021 [\[127\]](#), estableciendo una especie de “depósito en garantía” que cada validador debe depositar para poder agregar datos [\[128\]](#). Si comete

fraude, perderá el depósito.

Dejando –de momento– de lado las especificidades de los protocolos PoW y PoS, lo cierto es que la *blockchain* usa los protocolos de consenso como un mecanismo para asegurar que la información en ella inscrita sea siempre correcta [\[129\]](#), y se ha llegado a sostener que, puntualmente en PoW, el proceso de minado es una clara (y aparentemente útil) muestra de una estrategia de *gamificación* [\[130\]](#).

También se ha sostenido que los mecanismos de consenso de la *blockchain* permiten hablar de una *trustless trust*, o de *trust-by-computation* [\[131\]](#). La primera frase data de 2015 y corresponde a Reid Hoffman, el cofundador de LinkedIn, que antes fue Vicepresidente de PayPal y es uno de los más exitosos inversores de Venture Capital en el mundo [\[132\]](#). Hoffman sostenía, sin temor en 2015, que Bitcoin funciona, simultáneamente, como una moneda, un activo y una plataforma, por lo cual debiera ser bautizada como una *Global CryptoCAP (Currency, Asset, Platform)*. Esta *CryptoCAP*, siempre según Hoffman, es muy novedosa porque distribuye la responsabilidad de validar transacciones en una amplia red de nodos, llamados mineros, eliminando al costoso tercero de confianza, e.g. bancos y los procesadores de pagos, quienes hasta ahora eran los únicos encargados de autenticar y verificar los intercambios de valor *online*. Pero, más importante, permite “programar al dinero” y verá nacer otras muchas aplicaciones que hoy aún no se han inventado, todo sobre la base de la confianza descentralizada en la plataforma. Hoffman también afirmaba que como ningún gobierno u empresa controla la plataforma, los desarrolladores de software pueden innovar libremente y, como no existirán más de 21 millones de bitcoins, según Hoffman, es el Oro 2.0, pero mucho más divisible –un bitcoin puede partirse en 100 millones de veces–, es portable, y más verificable que cualquier moneda *fiat*, y, además, se valida en 10 minutos, cuando cualquier otra forma de pago on line puede demorar hasta días.

Trust by computation es una frase acuñada por Andreas Antonopoulos [\[133\]](#), e implica que en *blockchain*, la confianza *en la red* es asegurada requiriéndoles a los participantes que demuestren su poder de cómputo vía PoW. Esto implica que no hay que confiar en ningún actor o

participante de la red; no es necesario confiar *en personas* –o instituciones formadas por personas–, sólo debe confiarse en la matemática asociada a (o requerida por) los problemas que deben ser resueltos bajo un protocolo de PoW. Señala con razón Antonopoulos que llevará tiempo para que esta confianza descentralizada y computarizada se ponga de moda, ya que los sistemas de confianza centralizada llevan siglos de uso y existe una percepción general de que son el único sistema posible de confianza.

A modo de síntesis, se ha sostenido que se combina la criptografía, sumada al reemplazo de la confianza en un actor determinado por una confianza en una red de actores –en Bitcoin, los mineros– que son responsables por verificar las transacciones. En lugar de confiar en un Rey, el poder se distribuye en la gente, que lo expresa a través del voto de manera indirecta, eligiendo representantes –los mineros–^[134]. Y para ser minero, hay que invertir mucho, ya que cada problema matemático que debe resolverse en el PoW es cada vez más difícil, con lo cual se desincentiva el riesgo de mineros deshonestos^[135].

1.1.8.2.2. Cambios en el protocolo

Se ha planteado que es difícil cambiar el protocolo de consenso estipulado en una *blockchain* una vez que ya está funcionando, ya que los sistemas que tienen mecanismos bien estructurados para considerar e implementar cambios en el protocolo de consenso no son esencialmente descentralizados^[136].

En el caso de Bitcoin, existen los *Bitcoin Improvement Proposals*, BIPs, que permiten que los mineros hagan pública su voluntad o intención de establecer cambios al protocolo de *blockchain*, conocido como Bitcoin Core^[137] (BIP 9)^[138]. Uno de los BIPs, el BIP 91^[139] estableció un sistema de votación para cambios o actualizaciones en Bitcoin: si el 95% del *hash power* de la red declara aceptar un cambio dentro de un plazo determinado de tiempo, el cambio se vuelve obligatorio y debe implementarse. Este mecanismo se activó, por ejemplo, para aprobar e implementar el SegWit upgrade^[140] en

2017, un *soft fork* propuesto como BIP 141^[141] enfocado en problemas de escalabilidad de la red de Bitcoin, que dio lugar a la práctica conocida como UASF, *user-activated soft fork*^[142], y que permitió optimizar –aumentar, de facto– el espacio dentro de cada bloque (que tiene una capacidad de 1 MB), y a la vez aumentar la cantidad de transacciones por segundo, ya que cada bloque ahora contiene más transacciones dentro suyo^[143] y, a la vez, reducir más de 10 veces el costo de cada transacción por el mayor volumen transado.

El caso de Ethereum, la otra *blockchain platform* más utilizada en 2020, como se verá más abajo en § 1.9.1.1, cada vez que fue necesaria una modificación del protocolo –*soft* o *hard forks*–, demostró ser una situación de extrema gravedad y de gran impacto en el valor percibido de su crypto nativa^[144], el *Ether*, y del volumen de DAPPs usándola como *gas*^[145]. Tal y como se verá a su turno, lector, el hecho curioso que protagonizó *TheDAO*^[146], el *first-of-class* ente digital Ether-dependiente, que de tocar la guitarra eléctrica pasó a tocar el arpa en tan poco tiempo, puso en escena interesantes discusiones morales (y legales), y terminó costando el uso de la fuerza mediante un *hard fork*.

Es evidente, entonces, que quien mejor resuelva el delicado y humano problema de la cooperación adaptativa en el ámbito de las *BaaS platforms*, se queda con todo (o con mucho). Es aquí interesante referenciar el *problem-solution-fit* que se propone –recordar, cómo acordar cambios al protocolo de una *blockchain*– desde el equipo de Tezos^[147]. Tezos propone una *democracia líquida* –desconoce el autor si por influencia zygmuntiana– donde existe un *delegated PoS*, un derecho a votar que es libremente cesible, *proxy-friendly*. Quien tenga un token de Tezos, puede ser validador^[148]. Con quirúrgica precisión, el prestigioso profesor de Derecho del Wharton School, Kevin Werbach, afirma que los sistemas de gobierno *on-chain* hacen que la blockchain opere como cualquier otro sistema humano de gobierno, lo que no es perfecto. Remata citando a Churchill: es, sin embargo, la mejor opción posible entre un conjunto de malas opciones^[149].

1.1.8.2.3. Registro inmutable (¿y GDPR?)

La última y usualmente reconocida “característica esencial” de la *blockchain* –i.e., de algunas plataformas de *blockchain* determinadas–, es su inmutabilidad. Sin dudas, una característica bastante discutida [\[150\]](#), que ha quedado en un limbo regulatorio ante las regulaciones que han establecido un derecho al olvido absoluto, como el caso de Europa con su GDPR (y también el caso de Argentina, por cierto).

Con carácter de dogma, si las (una) *blockchains* deben poder o no ser editadas, es la pregunta causante del cisma entre los criptoentusiastas. En efecto, se ha afirmado que China *de facto* o *manu militari* podría, si quisiera, controlar el poder de cómputo necesario para revertir anotaciones en Bitcoin, sin mucho esfuerzo [\[151\]](#). Para añadir confusión, nótese que la conversación sobre mutabilidad o inmutabilidad tiene un significado muy distinto, dependiendo si se piensa en modificar costosas *blockchain* públicas (Bitcoin, Ethereum), o en modificar *blockchains* privadas –las precisas diferencias entre públicas y privadas se estudian más abajo en § 1.1.9. Las *blockchains* privadas pueden ser programadas *taylor-made* para grandes empresas, consorcios de empresas, o gobiernos. Existen interesantes casos exitosos de *techno-push*, el mejor, quizás es Hyper Ledger, impulsado por Fundación Linux desde 2015, con un *Governing Board* compuesto por 32 miembros, donde están representados incumbentes del *blockchain market*, pero también Universidades de prestigio internacional, empresas de tecnología Fortune 500, bancos de primer y segundo piso, empresas de software de negocios, entre otros [\[152\]](#).

Entonces, la inmutabilidad del registro distribuido *on-chain* es un punto esencial de las *blockchains*, que tiene interesantes vicisitudes asociadas. El asunto se dificulta aún más, si la legislación obliga a una *blockchain* a poder borrar un registro en ella contenido. Este es el caso de la Directiva Europea de Protección de Datos, o *GDPR* [\[153\]](#) en inglés, que empezó a regir en 2016, entrando en vigor a nivel doméstico en cada país de la Unión en 2018 [\[154\]](#). En ella se consagra el derecho al olvido a favor del consumidor, norma

también consagrada en Argentina bajo ciertas condiciones ^[155]. En este sentido, vale traer a colación que Accenture recientemente patentó una *blockchain* privada y editable muy interesante, que introduce el concepto del hash camaleón ^[156].

1.1.9. Tipos de *blockchains*

Se ha desarrollado una clasificación popular de las *blockchains* en públicas o abiertas, y privadas o permissionadas, incluyendo un *tertius genus*, las *blockchains* híbridas, que combinan aspectos de las abiertas y de las cerradas. Se seguirá el esquema de HACKERNOON, desarrollado por Nikolaos Kostopoulos ^[157]:

Imagen 5: clasificación *blockchains*

Positioning	Public Blockchain	Private Blockchain
Problem Statement	How to build an unstoppable X which is not managed by centralized entities.	How do I make business more efficient & compliant.
Network Participation	Unrestricted block creation Validators	Gated Participation/Restricted Roles
Participants' Identities	Unknown by default	Linked to known identities
Throughput	Network-wide bottlenecks	Scalable throughput
Governance	Open governance tools like DAOs- smart contracts and digital communities	Governance by a known entity
Network Fees	Fluctuating depending on demand for the network/gas fees	Contract which is dependent on the "consumption"
Popular Platforms	Ethereum, Cardano, Harmony	HyperLedger, Ripple, Ethereum Express Coin

1.1.9.1. Abiertas

Señala Schrepel^[158] que las *blockchains* públicas permiten acceso libre a cualquier persona que tenga acceso a Internet, y toda la información en ellas contenida es parte del dominio público, ya que cualquiera puede acceder a los datos *en ella*, aunque sin ser usuario *de ella*. Este atributo es conocido como el *Ojo Público*^[159], nadie requiere un permiso de acceso, ni una autorización ni una membresía. En efecto, cualquiera pueda ver el historial completo de transacciones de Bitcoin –la primera *blockchain* pública– aunque nunca haya adquirido ni un Satoshi, i.e. la unidad de medida equivalente a 0,00000001 Bitcoin. Cualquiera puede ser un nodo minero y mantener una copia del registro distribuido^[160].

En este tipo de *blockchains*, todas las transacciones registradas y asociadas a una determinada llave pública son transparentes para todos los participantes^[161]; el software subyacente es *open source* y está disponible para su descarga gratuita por cualquier persona interesada. Téngase en cuenta que en el caso de Bitcoin, su *blockchain* sólo registra transacciones no reversibles.

Se han señalado cinco características de estas *blockchains* públicas:

- (1) incluyen un protocolo para enviar, recibir y almacenar valor;
- (2) cuentan con “*Internet Value Containers*” –*coins* o *tokens*, que no son términos sinónimos–;
- (3) incentivos para el esfuerzo colaborativo;
- (4) software con licencia *open source* y mecanismos de gobierno; y
- (5) inmutabilidad del sistema^[162].

Las *blockchains* públicas más relevantes son Bitcoin^[163] y Ethereum. El caso de Ethereum merece especial atención. Se trata de una *blockchain* pública cuyo desarrollo inició en 2013^[164], 5 años después del lanzamiento de Bitcoin, de la mano de Vitalik Buterin, un programador de nacionalidad

rusa, criado en Canadá, i.e., un verdadero genio y crack de la programación, enamorado de Bitcoin y fundador de la Bitcoin Magazine [\[165\]](#). Lo acompañaron Mihai Alisie, Anthony Di Lorio y Charles Hoskinson, y juntos, proponían una Criptomoneda 2.0 (Bitcoin siendo la 1.0) [\[166\]](#).

Ethereum fue concebida como una *blockchain* pensada para algo más que simplemente registrar transferencias de titularidad de bitcons, al incluir un lenguaje de programación de tipo *Turing complete*, que permite que esta *blockchain* ejecute distintos tipos de programas, y a donde cada nodo de Ethereum tiene un protocolo que le permite operar una computadora virtual –*Ethereum Virtual Machine*, o EVM–. La EVM permite ejecutar los programas que se desarrollen para ella, y son llamados *Smart Contracts* [\[167\]](#). Para proteger la EVM del *spam* –i.e., cualquiera que tenga conocimiento en *Solidity*, el lenguaje de programación de Ethereum, puede desarrollar un programa para que corra en Ethereum–, los usuarios de Ethereum deben pagar [\[168\]](#) por cada paso que el programa ejecuta en Ether (ETH), la criptomoneda nativa de Ethereum.

Cinco años después, en 2018, Ethereum ya estaba en la boca y la cabeza de todo el mundo como la segunda *blockchain* pública más utilizada, después de Bitcoin. Operando desde una Fundación inscrita en Suiza, se fundeó el desarrollo de la plataforma emitiendo una moneda propia, llamada Ether, que recaudó 30.000 bitcoins en 2014, habiendo vendido 60 millones de Ether [\[169\]](#).

Al momento en que se escriben estas líneas, en plena cuarentena por COVID-19, mediando Abril de 2020, 1 Ether equivale a 160 U\$D, hay en circulación 110 millones de Ethers, y en conjunto representan un valor de mercado de 17.5 Billones de Dólares. El 1 de Diciembre de 2018 1 Ether llegó a valer 1.399 U\$D [\[170\]](#). El “canal B2B” de Ethereum, la *Ethereum Enterprise Alliance* (EEA), se lanzó a fines de 2017 [\[171\]](#) y nuclea empresas de primera línea mundial de todo tamaño y tipo [\[172\]](#) que la utilizan para experimentar nuevas aplicaciones de la *blockchain* a nivel corporativo.

Sin embargo, queda mucho camino por recorrer. Como uno de los

desarrolladores estrella de Ethereum, Vlad Zamfir, alguna vez dijo: *las blockchains son poderosas tecnologías con el potencial de causar un daño enorme. Y, también, de resolver serios problemas globales* [\[173\]](#). Y seguidamente remató con algunas afirmaciones complicadas: Ethereum no es segura; nadie puede garantizar que está libre de un ataque mayoritario como el que se describe en el próximo apartado; nadie puede garantizar que un *Smart Contract* se comportará tal como se esperaba; no es una plataforma escalable, y en esto, toda *blockchain* pública tiene el mismo problema [\[174\]](#).

Finalmente, debe destacarse que comienzan a desarrollarse *blockchains* públicas para fines determinados, que son permissionadas, y en las cuales cualquier persona puede *ver* la información, pero sólo participantes autorizados pueden *escribir* nueva información o desplegar contratos inteligentes. Un ejemplo de este tipo de *blockchains* es Sovrin [\[175\]](#), enfocada en el desarrollo de la tecnología de *SSID*.

1.1.9.1.1. El riesgo operacional de las *blockchains* públicas

Angela Walch ha investigado a fondo el llamado *riesgo operacional* [\[176\]](#). En un brillante y muy citado artículo señala varios puntos que son críticos y deben ser ponderados, así como Zamfir lo hizo respecto de la otra gran *blockchain* pública, Ethereum.

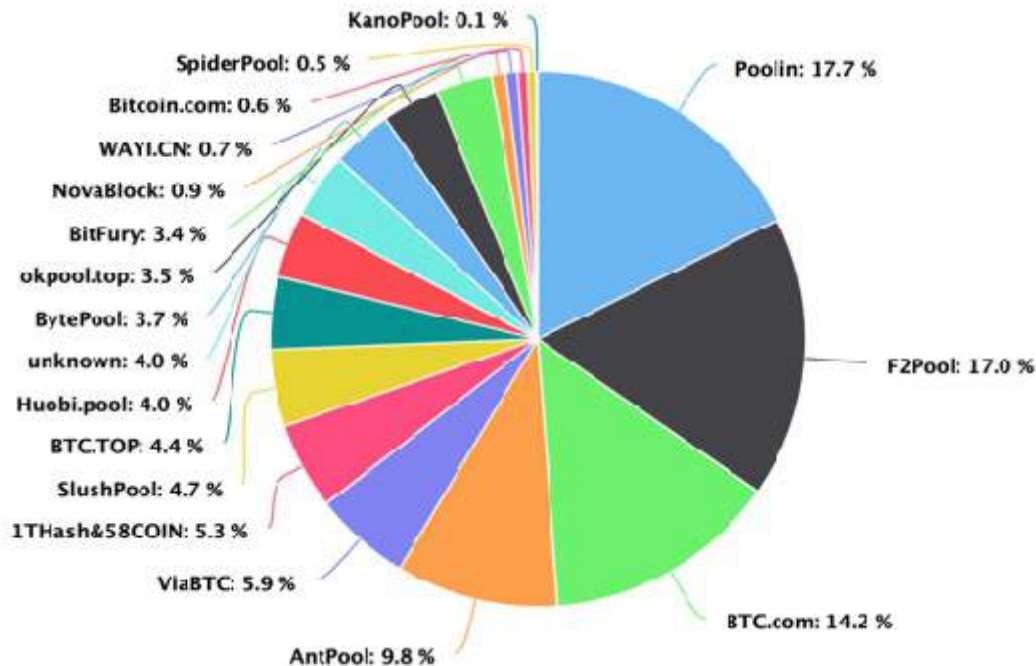
En efecto, Walch precisamente señala que el carácter de software *open source* [\[177\]](#) y descentralizado de Bitcoin la vuelve inapta para funcionar como infraestructura subyacente para los mercados financieros, ya que no hay una autoridad central que esté encargada de corregir o arreglar fallas *-bugs-* del software; aunque existe de facto un selecto grupo de programadores que se ocupan de desarrollar mejoras y mantener el software de Bitcoin, y que tienen el poder de enviar mensajes de emergencia a todos los nodos de la red, y decidir qué mejoras o cambios se implementan [\[178\]](#). En este sentido, se afirma que todo software tiene fallas, siempre [\[179\]](#); además es vulnerable a ataques [\[180\]](#), necesita ser actualizado mediante nuevas versiones [\[181\]](#) y muy

poca gente tiene la aptitud técnica de comprender qué significa todo lo anterior [\[182\]](#).

Puntualmente en relación a Bitcoin, se ha sostenido que es posible un “Ataque del 51%”, entendido como aquél realizado por nodos que controlen, al menos, el 51% del poder de cómputo de Bitcoin, o incluso menos, bastando un 30% del poder de cómputo o incluso menos si los mineros se ponen de acuerdo en afectar la cadena de bloques de los bitcoins [\[183\]](#). Buterin, en 2014, publicó un artículo sosteniendo que este tipo de ataque ya había ocurrido una vez en Bitcoin en 2013, con lo cual no es un mero ejercicio intelectual [\[184\]](#).

Al momento de escribir estas líneas, los grandes mineros del mundo se agrupan en *pools*, que se reparten los *block rewards* en proporción al *hashing power* aportado al pool [\[185\]](#). A marzo de 2020, el 81% de los pools de minado se encuentran en China, o lo que es lo mismo, China controla el 81% del *hash rate* en Bitcoin [\[186\]](#). El cuadro [\[187\]](#) abajo muestra la composición actual de los pools de minado:

Imagen 6: industria de minado



Por otro lado, los mineros no están exentos de ataques del tipo *Distributed Denial of Service* (DDoS), que puedan afectar el funcionamiento de Bitcoin. De hecho, esto ya ha pasado antes [\[188\]](#). La computación cuántica también puede poner en riesgo a Bitcoin, afirmándose que entre 5 y 10 años, *Sycamore*, la computadora cuántica de 64qubits de Google, podrá romper el encriptado de Bitcoin [\[189\]](#), a menos que el software sea actualizado para hacerlo *quantum-resistant* [\[190\]](#).

Como conclusión en relación al riesgo operacional de Bitcoin, reténgase que como todo software, Bitcoin es vulnerable a *bugs*, a ataques (internos, por parte de una cantidad relevante de mineros mal motivados, y externos vía DDoS), a la actualización no consistente de nuevas versiones, y a la dificultad de adoptar decisiones por no depender de una entidad, al ser un software descentralizado y *open source*.

1.1.9.1.2. El (supuesto) riesgo del autoritarismo on-chain

Existen quienes creen que el riesgo operacional de la *blockchain* no es el preocupante, sino que el mayor peligro de esta tecnología es el autoritarismo [\[191\]](#). Mientras estas líneas se escriben –en cuarentena por COVID-19–, llegan noticias desde Asia, sobre cómo la privacidad ha cedido espacio e importancia, en aras del control de la salud pública. El mundo mira con atención al experimento chino de los créditos sociales, que ya estaba en fase de testeo antes de la pandemia [\[192\]](#), y comienza ahora a unir puntos: masivas inversiones en esta tecnología, tanto a nivel público, como de inversores privados chinos, desde 2017 [\[193\]](#). Se ha afirmado que con un poco de programación, la *blockchain* puede ser diseñada para funcionar como un sistema de créditos sociales, y al combinarse con 5G, IoT, drones autónomos, tecnología de vigilancia, sistemas de reconocimiento facial, e Inteligencia Artificial, puede llevarnos a una esclavitud 2.0 [\[194\]](#).

Es interesante leer el *Blockchain White Paper* preparado por la Academia China de Tecnologías de la Información y la Comunicación, elaborado en 2018 [\[195\]](#), sumado a ello considerar que China tiene ya 500 proyectos que aplican *blockchain* [\[196\]](#), y vincular todo ello con la declaración del Presidente Xi Jinping en Octubre de 2019 afirmando que China debe aprovechar las oportunidades que *blockchain* le presenta [\[197\]](#).

1.1.9.2. Privadas

También llamadas permisionadas, a diferencia de las públicas, son aquellas cadenas de bloques en las que la información sólo es visible y accesible para ciertos usuarios autorizados, pudiendo incluso establecerse distintos grados de “visibilidad” según cada tipo de nodo/usuario, o permitirse visibilidad total. En efecto, un nodo puede ser una computadora de una entidad gubernamental, con determinados derechos de acceso a la información [\[198\]](#). A su vez, los permisos para agregar nueva información están centralizados por alguna entidad en función de determinados criterios, como Know Your

Customer (KYC) y Know Your Business (KYB). La principal diferencia con las *blockchains* abiertas es el grado de descentralización y anonimato que las privadas permiten [\[199\]](#). Se ha sostenido que una *blockchain* privada que no recurra a un protocolo de PoW sólo es un registro distribuido, pero no una cadena de bloques [\[200\]](#).

En alguna medida, en las *blockchains* privadas hay ciertos elementos de centralización, ya que se requiere permiso para poder utilizar la plataforma, ver la información contenida, y/o agregar bloques. En igual medida, estas *blockchains* están expuestas a riesgos de ciberataque similares a los sistemas centralizados [\[201\]](#). Estas cadenas privadas tienen un administrador que concede permisos, y pueden ser totalmente privadas (para uso de una sola empresa) [\[202\]](#) o consorciadas, mucho más comunes, en las que un conjunto de empresas que usan la *blockchain* para sus propios fines [\[203\]](#). Los casos más conocidos de *blockchains* consorciadas son HyperLedger, Quorum [\[204\]](#), TradeLens [\[205\]](#), Ripple y R3 [\[206\]](#), y un ejemplo de *blockchain* totalmente privada es la de Walmart [\[207\]](#).

Por otro lado, en estas *blockchains* privadas no es frecuente que se emitan criptomonedas, porque su diseño está orientado a que determinados participantes, normalmente empresas privadas o gobierno, transmitan o compartan información sobre transacciones o determinados eventos en único registro seguro y compartido [\[208\]](#).

Dentro de las *blockchains* consorciadas, sin dudas el caso más resonante es HyperLedger [\[209\]](#). A instancias y bajo la supervisión de la Fundación Linux, grandes empresas de tecnología –entre ellas IBM, Cisco, Intel– y de servicios bancarios –entre ellas, London Stock Exchange Group, JP Morgan y Wells Fargo– se unieron para desarrollar una *blockchain open source*, consorciada y multisectorial, enfocada al mundo de los negocios [\[210\]](#). A enero de 2020, ya cuenta con 250 miembros, y 15 proyectos activos.

1.1.9.3. Híbridas

Entre las *blockchains* públicas y privadas, existe un espacio de creación de nuevos formatos que pueden ser catalogados como *blockchains híbridas*, de modo tal de utilizar los atributos de unas y otras, para diseñar un traje a medida del problema que se busca resolver. Quizás el caso más icónico del formato híbrido será Libra, analizada más abajo, y que nacería como una *blockchain* privada con vocación de convertirse en una *blockchain* pública en el futuro [\[211\]](#).

Es importante el futuro (y fértil) campo de acción de las *blockchains* híbridas en particular, y de las DLTs en general. Hasta el surgimiento de las DLTs, dos partes independientes sólo podían obtener y confirmar información vinculada a sus negocios a través de dos maneras: recurriendo a un servidor central, asumiendo que ambas partes acuerden respetar lo que el servidor informe –*consenso por autoridad*–; o chequeando la información del registro que cada parte lleva, y conciliando, reconciliando y así hasta acordar algún estado de información mutuamente aceptado –*consenso por reconciliación*– [\[212\]](#). Esto era así, hasta la aparición de *blockchain*, que propuso una tercera forma de confirmar un estado dado de información (o de valor) en único registro, a través de la criptografía, mecanismos de consenso y otras tecnologías. Pero la descentralización como atributo la *blockchain*, i.e., distribuir la información a todas las partes, genera dos problemas: por un lado, puede poner en riesgo la privacidad –y esto importa si los datos son sensibles, como en el caso de la salud y la banca– y, por el otro, a medida que crece la información alojada –más uso, escalabilidad–, decrece la velocidad del sistema [\[213\]](#). Estos problemas generarán, con el tiempo, que se multipliquen los modelos híbridos, que recurren a atributos de las *blockchains* privadas y públicas, según la necesidad del caso o de cada *problem-solution-fit*.

1.1.9.4. Otras clasificaciones

Christidis y Devetsikiotis^[214] proponen una interesante clasificación que también es muy didáctica, dependiendo de:

1) Quién puede acceder a la *blockchain*?: Si cualquier persona puede acceder, es una *blockchain* pública. Si sólo algunas personas determinadas pueden acceder, es una *blockchain* permissionada. En las *blockchains* públicas, los protocolos de consenso son hasta ahora costosos (e.g., PoW) y son necesarios ciertos estímulos económicos para los nodos mineros que mantienen y actualizan el registro (e.g., una criptomoneda, bitcoin, ether, etc.). Las *blockchains* privadas pueden ser más adecuadas para casos en los que se necesita un entorno controlado, regulado.

2) Quién puede transaccionar o minar (e.g. agregar bloques nuevos) o iniciar contratos inteligentes en la *blockchain*?: En las *blockchains* privadas, puede haber muchos tipos de permisos. MultiChain, por ejemplo, tiene ocho permisos distintos, y cada uno permite realizar distintas acciones^[215]. En las *blockchains* públicas, generalmente cualquier persona puede ser un nodo y realizar las actividades que la *blockchain* permita.

3) ¿Es una *blockchain* con arquitectura UTXO^[216] o *account-based*^[217]?: En las *blockchains* públicas más populares, Bitcoin usa el modelo UTXO y Ethereum usa el modelo *account-based*.

1.1.10. La evolución de la Blockchain

Schreppel^[218] sostiene que se pueden distinguir tres momentos en la

evolución de la *blockchain*:

1) *Blockchain 1.0*: es el primer estadio de la *blockchain*, donde se la utiliza exclusivamente vinculada a criptomonedas, a transferencias de criptomonedas como bitcoins, a nuevas formas de envío de dinero y como sistema digital de pagos.

2) *Blockchain 2.0*: es el segundo estadio de la *blockchain*, donde se la utiliza como una especie de contrato, que puede utilizarse en relación a variados objetos: acciones, bonos, préstamos, contratos de futuro, hipotecas, inversiones, crowdfunding, y en general, toda clase de *Smart Contracts* y smart property. En una primera instancia, aparecen los contratos tipo Dapps ^[219]; en una segunda instancia aparecen las DOS ^[220] y los DAOs ^[221] ^[222] que ya cuentan con una especie de constitución que codifica sus reglas para que todos los interesados puedan verlas y aceptarlas, incluyendo las DACs ^[223], que son DAOs bajo una forma particular de organización legal; y en tercera y última instancia, aparecen las DAS ^[224], que combinan todos los anteriores.

3) *Blockchain 3.0*: este estadio en la evolución de la *blockchain* “exporta” sus bondades a otros sectores no tan vinculados a los servicios financieros, hacia el área del gobierno, la cultura, el arte, la salud, la ciencia y la literatura.

Evidentemente, la *blockchain 2.0* genera interesantes debates para el Derecho, y es el motivo por el cual este Manual se escribe.

En efecto, y puntualmente en relación a las DACs, *decentralized autonomous corporations*, se ha señalado que la *blockchain* permitirá directamente iniciar una nueva era en la forma de organizar negocios.

Así, se espera que surjan las DACs, empresas que son directamente codificadas en la nube, basadas en algoritmos, configuradas para realizar

ciertas actividades que crean valor [\[225\]](#). Incluso se sostiene que Bitcoin –el protocolo, no la moneda– es, de hecho, una DAC *per se*:

- i) su código corre en los nodos de la red;
- ii) cualquiera que tenga un bitcoin, es un “accionista”;
- iii) los “dividendos” se distribuyen proporcionalmente, en forma de *black rewards* a los mineros; y
- iv) tiene un sistema de gobierno –corporativo– *on-chain* que es el protocolo de PoW, por el cual los mineros pueden votar en la medida que contribuyan al mantenimiento de la red, incluso podrían votar en contra y dividir la cadena –sería el equivalente a un derecho de receso– [\[226\]](#).

Sacando el caso puntual de Bitcoin como DAC, se ha sostenido que una DAC es una sociedad que vive en la nube, y que realiza funciones valiosas para sus clientes, a los que automáticamente se cobra por los servicios brindados, pudiéndose automatizar los pagos vía Dapps.

Las DACs dividirán –programarán– las tareas, dividiéndolas entre las que son repetitivas y triviales, y pueden ser automatizadas mediante software; y las que requieren actividad creativa, innovación, o gestión de crisis, tareas que no pueden ser ejecutadas por computadoras, pero sí por humanos calificados que serán atraídos por incentivos, y contratados por la DAC.

El código que gobierne todas estas acciones no podrá ser modificado sin alcanzarse una mayoría determinada de usuarios o de accionistas, y tal código será públicamente divulgado [\[227\]](#). Evidentemente, los órganos de administración naturales no parecerían ser necesarios, ya que el código ha sido programado para tomar decisiones usuales de negocios, o podría integrarse el código programado con una Inteligencia Artificial entrenada específicamente en un campo de negocios particular [\[228\]](#).

No es temerario afirmar que esta es la primera vez en la historia de la Humanidad que una tecnología, que está en su infancia, permitirá estructurar negocios de este modo [\[229\]](#).

GARTNER, por su parte, propone un espectro de casos en la utilización de la *blockchain* [\[230\]](#) donde identifica la siguiente evolución en tres fases:

(i) *blockchain-inspired*: desde 2012 a 2020, donde las soluciones de *blockchain* solo usan tres atributos: distribución, encriptado e inmutabilidad y hay mucha experimentación;

(ii) *blockchain-complete*: muy apalancada en la tokenización, en dotar de liquidez a activos ilíquidos y en los *Smart Contracts*, esta etapa tomará probablemente hasta 2025 en desarrollarse; y, finalmente,

(iii) *enhanced-blockchain*: a partir de 2025, otras tecnologías como IoT, IA y SSID se combinarán con las plataformas de *blockchain*, permitiendo microtransacciones entre objetos autónomos y computarizados, sin intervención humana y la utilización creciente de DAOs.

1.1.11. Grupos de interés

Debe resaltarse también la formación de muchísimos grupos de interés que se dedican a promover la *blockchain* o sus aplicaciones.

Entre éstas, debe destacarse el rol de Alastria en España, una asociación sin fines de lucro que fomenta la economía digital a través del desarrollo de DLTs y de *blockchain* [\[231\]](#). Alastria ofrece a sus socios dos redes operativas (Red T y Red B) sobre las que pueden desplegarse nodos (bien nodos regulares o bien nodos críticos validadores y permisionadores). La Red T está construida sobre tecnología Quorum y la Red B sobre Hyperledger Besu. Como plataforma *blockchain* “agnostic”, Alastria no confía su desarrollo a una sola plataforma, y por ello se han iniciado trabajos de creación de otro tipo más de red basada, en HyperLedger Fabric (de The Linux Foundation) y en cómo interconectar las tres redes y con otras redes en el futuro [\[232\]](#).

También en Europa, la Comisión Europea creó en 2017 el

OBSERVATORIO Y FORO DE *BLOCKCHAIN*^[233] con la finalidad de monitorear las actividades Europeas en *blockchain* y hacer recomendaciones a nivel comunitario. En 2018 se conformó la *European Blockchain Partnership*, en la cual treinta países europeos han acordado utilizar la *blockchain* para optimizar y hacer más eficiente los servicios públicos digitales *cross-border*^[234] desarrollando la *European Blockchain Services Infrastructure* (EBSI)^[235], enfocándose inicialmente en notarización, validación de títulos universitarios, una *Self-Sovereign-Identity* (SSI) europea^[236] y una ventanilla única para fines aduaneros y fiscales^[237].

También merece resaltarse el caso de la INTERNATIONAL ASSOCIATION FOR TRUSTED *BLOCKCHAIN* APPLICATIONS (INATBA), un foro internacional que reúne a más de 170 empresas, reguladores y *policy makers*^[238]. Del otro lado del Atlántico, existe la *Blockchain Advocacy Coalition* creada en 2019 para asesorar en el diseño de políticas públicas en el Estado de California^[239]. Por su parte, la International Standards Organisation (ISO) planea presentar en 2021 una serie de nuevos estándares para *blockchains* y DLTs, pensando en unificar terminología y garantizar la interoperabilidad entre una cantidad cada vez mayor de *blockchains* consorciadas^[240].

En Argentina, existe la ONG Bitcoin Argentina^[241] y la red *Blockchain Federal Argentina*^[242], que ofrece una plataforma multiservicios que corre sobre Ethereum, cuenta con distintos tipos de nodos, y permite su utilización gratuita para probar o desarrollar servicios y aplicaciones sobre la *blockchain*, a condición de aceptar un acuerdo de utilización y buenas prácticas, pero sin estar obligados a desplegar nodos selladores. En esta *blockchain*, el almacenamiento de información es *off-chain*, por lo que la plataforma no funciona como una nube para almacenar archivos, sino que cada servicio desplegado es responsable de los mismos. En el registro de esta *blockchain* sólo se almacenan los digests criptográficos (los *hashes*) de esos archivos, lo

que basta para garantizar que los mismos no han sido modificados [\[243\]](#).

1.1.12. Inversiones en blockchain en 2019

La encuesta anual de DELOITTE [\[244\]](#) sostiene que en 2019 el 53% de los ejecutivos encuestados confirmó que *blockchain* se había convertido en una prioridad en sus organizaciones, y señala que los países que llevan la delantera en la materia son China, Singapur e Israel.

En un muy interesante trabajo publicado en 2018 [\[245\]](#), desde el punto de vista de las startups enfocadas en *blockchain* y los sectores en los que operan, más del 75% de ellas operan en el sector de finanzas y seguros, e información y comunicación. Dentro de la categoría de finanzas y seguros, la mayoría de las startups que operan en *blockchain* en 2018 ofrecieron servicios de Exchange, trading, procesamiento de pagos, pagos y crowdfunding.

Imagen 7: inversiones en blockhain

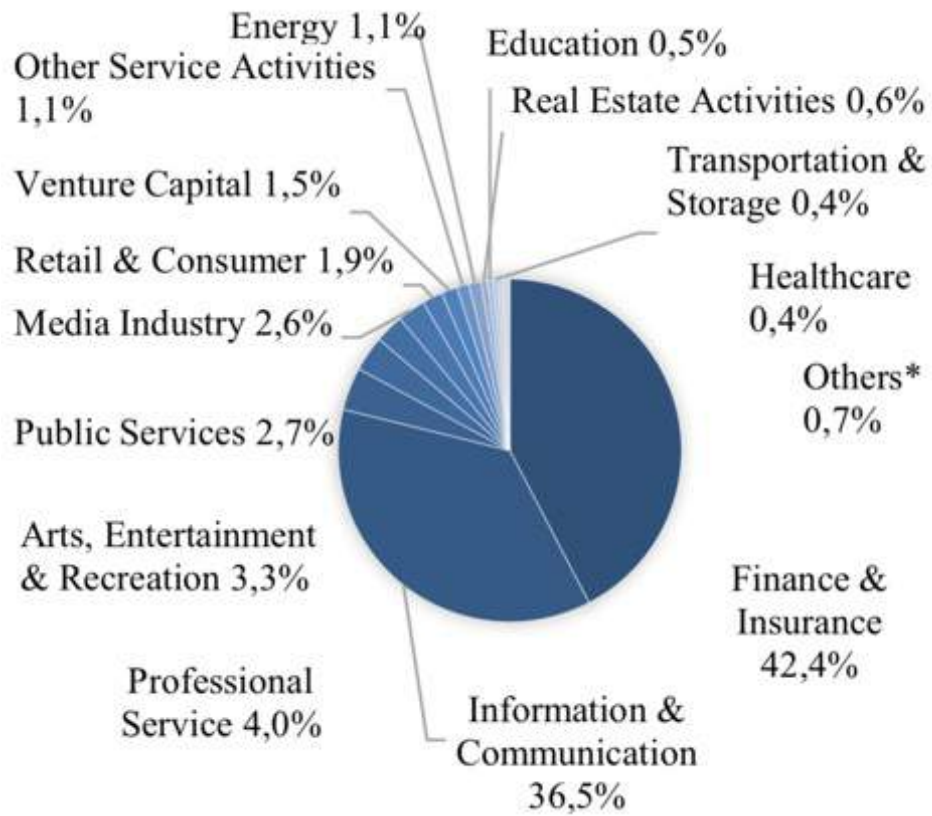
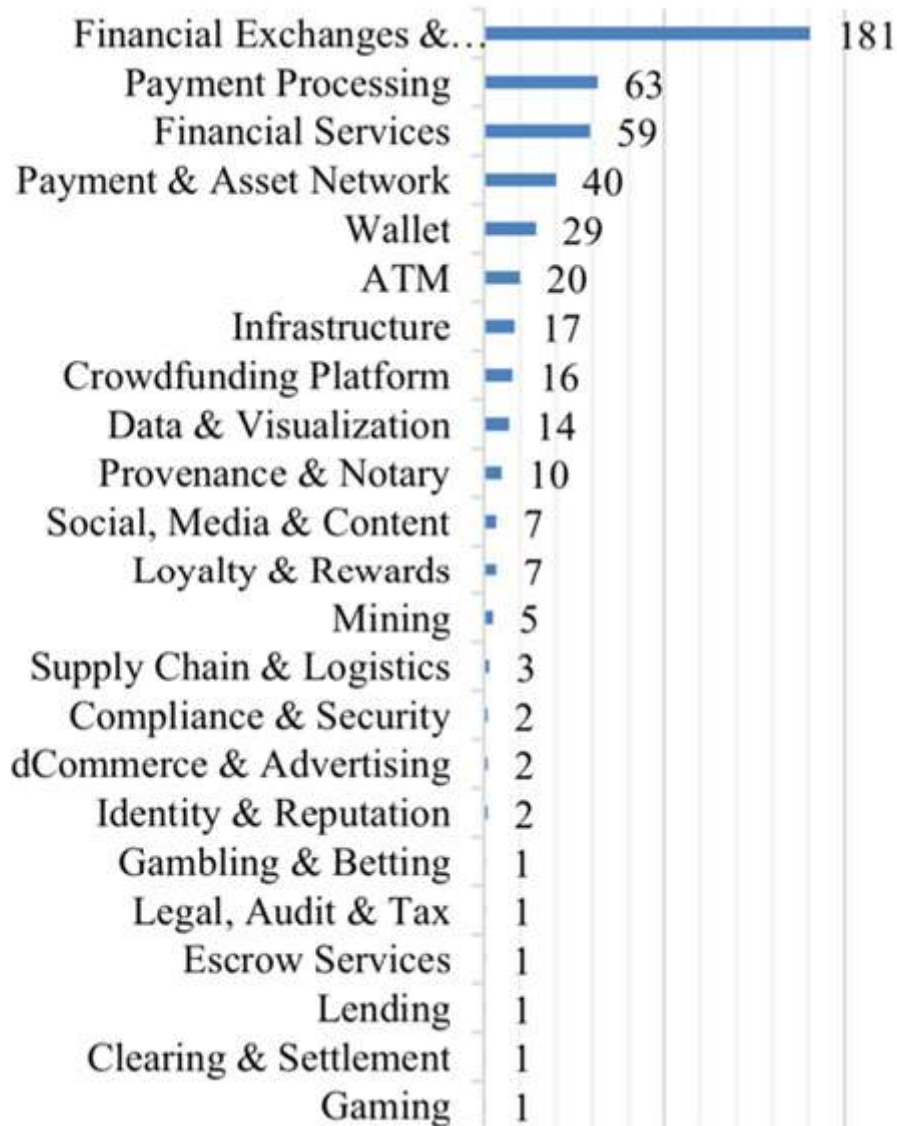


Imagen 8: segmento de servicios



1.2. Limitaciones de la Blockchain

En el apartado anterior de este Capítulo, se conceptualizó introductoriamente la tecnología *blockchain*, se presentaron sus antecedentes, sus varias deficiones, sus características, sus clasificaciones usuales, sus riesgos, y se hizo un paneo de los flujos de inversiones en los últimos dos años. Ahora es momento de analizar sus limitaciones, que al igual que sus virtudes, no son pocas pero deben ser conocidas.

Fulmer ^[246] indica que a pesar de ser una red descentralizada, existe un conjunto de individuos que están a cargo de mantener y desarrollar el código de Bitcoin ^[247], ya que como cualquier software, el de Bitcoin –y el de cualquier otra *blockchain*– debe ser actualizado, corregido y mejorado por alguien, a medida que la tecnología avanza. Esto implica que si hubiera una entidad encargada de mantener el código, sería un intermediario que podría asumir una posición de poder, e incluso, sin una figura central a cargo de ello –como es la situación actual–, pueden generarse controversias entre los programadores sobre si es o no necesario avanzar con una determinada modificación o mejora, y éstas controversias crecen a medida que crece el efecto de red, con más usuarios dentro de ella ^[248].

Por otro lado, sigue siendo una tecnología bastante difícil de entender para el mortal medio, sin estudios de programación. Hasta que no sea mayormente utilizada, mucha gente se mantendrá escéptica sobre su utilidad, principalmente porque no entienden cómo funciona y para qué puede servir. Tanto es así que se ha sostenido que como tecnología es como una solución que aún está buscando problemas para resolver ^[249]. Fulmer también puntualiza los problemas que puede generar el atributo de la inmutabilidad, y como una división de la *blockchain* –*hard fork*– para resolver algún dato mal ingresado –ya ha pasado en Bitcoin ^[250] y en Ethereum–, pero puede generar un problema adicional: que coexistan dos *blockchains* en lugar de una, corregida y mejorada, tal como ocurre con Ethereum en la actualidad.

Por otro lado, la posibilidad del “Ataque del 51%” sigue siendo real, e incluso ha pasado antes como ya se indicó ^[251] y podría pasar con menos *hashing power* ^[252]. Además, el avance de la computación cuántica también presenta riesgos para las técnicas de encriptado asimétrico de la *blockchain*, aunque avances rusos podrían despejar este riesgo ^[253].

Específicamente, el algoritmo para creación de llaves públicas conocido como *Elliptic Curve Digital Signature Algorithm*, ECDSA, podría ser afectado

por la computación cuántica a más tardar en 2027^[254], o antes, afirmándose que en 200 segundos, la supercomputadora cuántica de Google puede descifrar una llave privada hexadecimal de 64 dígitos, a menos que comiencen a utilizarse técnicas de criptografía *quantum-resistant*^[255].

Finalmente, se ha señalado que muchas patentes que son susceptibles de afectar el futuro desarrollo de la *blockchain* están pendientes de concesión en todo el mundo, y ello podría ser una limitación para la innovación y futuros desarrollos^[256].

1.3. *Cryptocurrency & Blockchain 1.0*

Innegable es que la *blockchain* como tecnología fundacional se hizo conocida por su vinculación a Bitcoin, y por la circulación “estable aunque volátil” de bitcoins. Circulan a abril de 2020 un poco más de 18 millones de bitcoins, siendo 21 millones la cantidad total de ellas que existirán^[257]. En este primer capítulo introductorio, donde se responden algunas *Frequently Asked Questions* –FAQs– de la *blockchain*, se darán también algunos conceptos esenciales sobre utilización más popular en la *Blockchain 1.0*: las llamadas criptomonedas, aclarándose que el estudio de la llamada CriptoEconomía^[258] y de la Token Economics^[259] excede ampliamente el objeto de este Manual, por lo cual sólo se abordarán cuestiones estrictamente vinculadas con los *Smart Contracts*.

1.3.1. *El Cryptomarket*

A partir de 2014, se comenzó a ver una ola de las llamadas *ICOs*, *Initial Coin Offerings* en el mercado primario, generalmente utilizando *blockchains* públicas. De hecho, la expresión *ICO* emula la frecuentemente utilizada para la emisión primaria de acciones, *Initial Public Offering*, *IPO*, y hace referencia a un evento de captación de fondos mediante la emisión en *blockchain* de *tokens* o *monedas digitales* que son ofrecidos a potenciales inversores, en

contraprestación por su inyección de capital en monedas convencionales, o *fiat currencies*, o también en bitcoins o Ether.

Las ICOs se anuncian en canales *on line* tales como foros de criptomonedas. Aún cuando toda ICO involucra criptomonedas, la ICO *per se* difiere de la emisión de una criptomoneda propiamente dicha, tal como bitcoin, ya que éstas no se emitieron para financiar una startup, y al menos en el caso de bitcoin, éstas se emiten en pago a los mineros –*black reward*– por una actividad muy puntual: el minado vía PoW ^[260].

Estos *tokens* o monedas digitales –*coins*– ofrecidos al público a cambio de la inversión en nuevos emprendimientos pueden ser considerados valores negociables ^[261] o títulos valores ^[262], dependiendo de la jurisdicción de que se trate ^[263], lo que será desarrollado en profundidad en el Capítulo III más abajo.

Ahora bien, además de las emisiones primarias de tokens, existe también un mercado secundario donde éstos son tranzados de manera directa y, esencialmente, sin intermediarios ^[264].

La expresión “*CryptoMarket*” involucra tanto a las criptomonedas de *blockchains* públicas (principalmente Bitcoin y Ether), como así también todas las ICOs emitidas en *blockchain*, su negociación secundaria, y la valuación de todo lo anterior. Al 16 de Abril de 2020, el *CryptoMarket* está compuesto por 5.356 monedas digitales, que “cotizan” en 21.367 mercados, con una valuación conjunta de U\$D 201.292.920.015 y un volumen de transacciones en las últimas 24 horas de U\$D 154.226.238.275, volumen del cual la negociación de bitcoins representó el 63,9% ^[265]. En su momento de máximo auge, entre Diciembre de 2017 y Enero de 2018, el *CryptoMarket* llegó a ser cuatro veces su tamaño actual pasando los 800 billones de Dólares de valuación ^[266], casi llegando al trillón de Dólares.

Este monstruoso mercado de monedas digitales es exclusivamente motorizado por emisiones privadas, en el sentido de que no hay ningún Gobierno atrás de ellas, salvo por el oportunismo fiscal de muchos Estados, que intentan capturar parte de esas apreciaciones a los fines fiscales, como

también se verá más abajo [\[267\]](#).

Sin embargo, la tendencia que se comienza a vislumbrar es la de los Estados estudiando fuertemente la conveniencia de emitir las denominadas *Central Bank Digital Currencies*, CBDCs, que a continuación se analizan. En efecto, el Banco de Canadá, el Banco de Inglaterra, el Banco de Japón, el Banco Central Europeo, el Banco de Suecia, el Banco Nacional Suizo, y el Banco de Pagos Internacionales han creado un grupo de trabajo sobre CBDCs [\[268\]](#).

El FMI también investiga la materia [\[269\]](#), afirmando que las CBDC pueden promover una mayor inclusión financiera, una mayor estabilidad y ofrecer menores barreras de entrada para nuevas empresas en el sistema de pagos, sin requerir que las personas tengan una cuenta bancaria.

Además, el FMI sostiene que las CBDCs pueden ser un medio para contrarrestar las nuevas monedas digitales: “una moneda digital emitida en el país respaldada por un gobierno de confianza, denominada en la unidad de cuenta doméstica, puede ayudar a limitar la adopción de monedas emitidas en forma privada (por ejemplo, stablecoins), que pueden ser difíciles de regular y pueden presentar riesgos para la estabilidad financiera y la transmisión de la política monetaria” [\[270\]](#).

1.3.2. CBDCs

Recientemente, el Banco de Inglaterra publicó un informe, *Central Bank Digital Currency: opportunities, challenges and design* [\[271\]](#), que se tomará de guía en este apartado. En el informe se indica que estamos en el medio de una revolución en las formas de pagar, y que las CBDCs serían una verdadera innovación, tanto en la *forma* del dinero provisto como en la *infraestructura subyacente* que moviliza y permite los pagos [\[272\]](#), y se propone a modo ilustrativo un posible diseño de plataforma de CBDC [\[273\]](#).

Con mucha precaución, el Banco de Inglaterra no se apresura en confirmar que una CBDC debiera utilizar tecnologías DLT, aunque reconoce que en caso de recurrir a la DLT, se obtendrían beneficios de la descentralización con

respecto a la resiliencia del sistema, así como el uso de *Smart Contracts* podría facilitar el desarrollo del *dinero programable* [\[274\]](#).

La precaución inglesa contrasta con la premura China, que viene testeando una CBDC desde 2017 utilizando *blockchain* [\[275\]](#) y, se descuenta, lanzará el *Yuan Digital* en 2020 en plena crisis global por la pandemia del COVID-19 [\[276\]](#).

Sin dudas, cuando el lector esté leyendo estas líneas, China ya habrá llevado a la realidad su CBDC, en la cual colaboraron Alibaba, Tencent, Huawei y el China Merchants Bank, participando activamente en el desarrollo de la moneda digital, con Alipay de Alibaba y WeChat Pay de Tencent aglutinando en conjunto más de 1,700 millones de cuentas activas en toda China, 300 millones más que la población del país [\[277\]](#). Esta colaboración público-privada para dar forma al *Yuan Digital* puede ser enmarcada en el ODS #17, y ser quizás una de las mayores aplicaciones reales del mismo, hasta ahora. Se descuenta, también, que el Yuan Digital se integrará en el circuito de pagos de la Ruta de la Seda Digital que vincula a 130 países de todos los continentes [\[278\]](#).

Finalmente, es interesante tratar aquí el caso de Estonia [\[279\]](#), que ha propuesto lanzar tres tipos de *Estcoins*:

- i) un *community estcoin* que no tiene respaldo, y se lanzará como una ICO para recaudar fondos. Este *community estcoin* que sólo podrá ser acreditado a e-residents de Estonia, que pueden *ganar estcoins* realizando actividades como invitar a nuevas personas a que obtengan su e-residence, y que será aceptado por comercios de Estania;
- ii) un *identity estcoin*, que vincula la identidad digital de los e-residents con un token, como una forma de SSID para Estonia. Este token no es tranzable, y opera como un certificado de identidad digital para operar con community tokens y pueden ser cancelados en caso que los e-residents incumplan

obligaciones; y

iii) un *euro estcoin*, que es una *stable coin* pegada al Euro, y puede ser utilizado como medio de pago entre los e-residentes de Estonia. Este token puede comprarse pagando en Euros, y es convertible por Euros, al tipo de cambio que fija el Gobierno [\[280\]](#).

1.3.3. Libra

Finalmente, y quizás con un impacto potencial mayor al de muchas CBDCs agrupadas, no puede dejarse sin analizar el caso de *Libra*, la criptomoneda de Facebook [\[281\]](#). En tan solo 26 páginas, escritas por 53 autores, Facebook presentó al mundo su idea de criptomoneda nativa el 18 de Junio de 2019 [\[282\]](#).

Lógicamente, Libra capturó la atención de políticos, reguladores y medios de comunicación de todo el mundo por la sencilla razón de que Facebook tiene, a fines de 2019, casi 2.5 billones de usuarios activos [\[283\]](#), con lo cual 1/3 de la población del mundo tendría su primer contacto con una criptomoneda, y probablemente la usaría.

Es interesante hacer este ejercicio de simulación (a valores a Abril de 2020):

- (i) el *market cap* de Facebook ronda hoy aproximadamente los 499 mil millones de Dólares (equivalente aproximadamente 1 PBI de Argentina); y
- (ii) si se asume –sólo por simular un ejemplo– que:
 - (a) el 70% de todos los clientes de Facebook usarán Libra a finales de 2021, ello representaría 1.75 billones de usuarios y el 22% de la población del mundo;
 - (b) cada usuario de Libra realizara al menos una transacción *por mes*, con un valor promedio de U\$S 30, y

asumiendo también que las comisiones por transacción de Libra fueran del 5%, i.e. U\$D 1.50, a finales de 2021, entonces Libra

(iii) sólo en un mes cualquiera transaccionaría aproximadamente U\$D 55.500.000.000 en volumen de transacciones (lo que equivale prácticamente al 10% de la valuación actual de Facebook), y generaría ganancias mensuales por unos 2.500 millones de Dólares, solo por el uso de Libra (y Calibra, su *Wallet* propia).

Ahora bien, siguiendo con el ejercicio de simulación,

(iv) si se asume que el restante 78% de la población mundial usaría Libra antes de 2025, entonces quizás en el 2026, cuando Libra ya sea una DLT abierta (o en proceso de convertirse en ello), el volumen anualizado de transacciones promedio y de comisiones (ganancias netas) generadas, podría llegar a ser, respectivamente, de U\$D 2.772.000.000.000 (poco más de 5 veces, 5x, la valuación actual de Facebook) y de U\$D 138.600.000.000 (la ganancia neta de Facebook, por todas sus líneas de negocio durante todo el 2019 fue de U\$D 7.349 millones [\[284\]](#), lo cual implicaría un múltiplo de ganancia neta de casi 18x para 2026, asumiendo que todo el mundo utilizará Libra).

Interesante negocio, que transaccionaría sobre *Smart Contracts* programados en *Move*, el lenguaje de programación de Libra.

Señala Schrepel que Libra sería, en sus inicios, una *blockchain* privada, i.e. permissionada, en la que solo determinados usuarios, por turnos rotativos, validarán las transacciones involucradas a través de un protocolo de PoS [\[285\]](#), pero aspira a convertirse en una *blockchain* pública en 5 años, asumiendo que, en el futuro, habrá una “proven solution that can deliver the scale, stability, and security needed to support billions of people and

transactions across the globe through a permissionless network”^[286].

Se dejan a continuación diez puntos sobresalientes de Libra:

- 1) Las transacciones estarán basadas en *Smart Contracts*, en un principio pre-definidos por Libra, y ulteriormente, definidos por cada usuario. El lenguaje de programación se llama *Move*^[287];
- 2) Moneda Estable: el valor inicial de Libra estará vinculado a una canasta de monedas convencionales^[288];
- 3) Los usuarios operarán con pseudónimos, ya que las cuentas no están vinculadas a la identidad real de las personas;
- 4) La plataforma utilizará un recurso para alimentar la validación, mediante un sistema parecido al gas en Etheruem, aparentemente^[289];
- 5) No empaquetará la información de las transacciones en bloques, como en Bitcoin o en Ethereum, y toda la información se almacena en un único registro distribuido, con lo cual Libra no es técnicamente una *Blockchain*, sino una DLT;
- 6) La plataforma cobra comisiones por transacción, denominadas en Libra *coins*;
- 7) La Asociación Libra controla la reserva de Libra *coins*, las que están respaldadas por monedas convencionales. La asociación puede emitir nuevas monedas si la demanda crece, y destruirlas si la demanda cae, pero sólo a solicitud de revendedores autorizados de las *coins*; y no se ampliará la cantidad de Libra *coins* si no se amplía proporcionalmente la canasta de monedas fiat que la sustenta;
- 8) Inicialmente, se utilizará una *wallet* propia, llamada *Calibra*, que verifica la identidad real, y hará los controles de AML-KYC;

- 9) Cualquier programador, cliente, empresa o usuario, podría desarrollar apps sobre la plataforma de Libra; y
- 10) Cualquier cambio a las reglas anteriores, requiere de un voto mayoritario de 2/3 de los miembros fundadores [\[290\]](#).

II. Smart Contracts: *FAQs*

2.1. Algunas definiciones (*fans vs. haters*)

Entendidos los principales antecedentes, el funcionamiento, las virtudes y las limitaciones del género de tecnologías denominadas *DLTs* y, especialmente, de su especie más popular, la *blockchain*, se propone ahora en este segundo Capítulo ahondar en las aplicaciones que más llaman la atención en la denominada *Blockchain 2.0*: los *Smarts Contracts*.

Al igual que en el caso de *blockchain*, abundan las definiciones sobre qué es un *Smart Contract*. En este primer apartado se pasará revista a las definiciones más importantes –incluyendo especialmente las visiones más críticas–; en el segundo apartado se analizarán las cuatro características esenciales de los *Smart Contracts*; en el tercero se analizarán casos concretos de aplicación actual, y en el cuarto y último apartado de este Capítulo, se desmitificará a los “contratos inteligentes”, hasta casi demostrar que, en su estado actual de evolución, son más bien *Dumb Contracts* ^[291] que sirven para automatizar algunas limitadas funciones, pero no sirven para otras muchas. Pero, no dude el lector que, sin dudas, evolucionarán *pari passu* a la masificación de la *blockchain* y a medida que ésta tecnología avance de la niñez hacia la madurez, a partir de 2025 en adelante.

Se empezará por el inicio, y así como el inicio de *blockchain* es asociado al icónico y desconocido Satoshi Nakamoto, los *Smart Contracts* son linkeados directamente a un paper de Nick Szabo subido en 1997 en su blog ^[292], aunque se ha afirmado que la relevancia práctica de los *Smart Contracts* era muy limitada hasta que surgió Bitcoin ^[293]. Szabo tiene dos títulos, Licenciado en Computación y Abogado, de allí que pueda vincular con mucha fluidez la Tecnología y el Derecho ^[294].

En la mente de Szabo, los *Smart Contracts* eran esto:

“Many kinds of **contractual clauses** (such as collateral,

bonding, delineation of property rights, etc.) can be **embedded in the hardware and software** we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of Smart Contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas. Smart Contracts go beyond the vending machine in **proposing to embed contracts in all sorts of property that is valuable and controlled by digital means**. Smart Contracts reference that property in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.” (el resaltado es mío) [\[295\]](#)

Y, acercándose a una definición, Szabo conceptualizaba los *Smart Contracts* a través de su función:

“Smart Contracts combine protocols, users interfaces, and promises expressed via those interfaces, to formalize and secure relationships over public networks [\[296\]](#)”

y los definía como:

“a computerised transaction protocol that executes the terms

of a contract”[297] [y como] “a set of promises, specified in digital form, within which the parties perform on these promises.”[298]

Ahora bien, la doctrina más contemporánea ha criticado fuertemente a Szabo y su definición. En efecto, la Profesora Eliza Mik, de la prestigiosa Singapore Management University sostiene que muchos *Smart Contracts* no son, en realidad, contratos en un sentido legal[299], reinando mucha confusión en la materia[300], y afirma que lo único que en realidad sí son, es un programa que se ejecuta en la *blockchain*. Es más, sostiene Mik que las publicaciones de Szabo contienen muchos errores, y que es necesario distinguir entre *Smart Contracts* en sentido tecnológico, y *Smart Contracts* en sentido legal, debiéndose aceptar que ésta última definición –más amplia– puede incluir a aquélla –más escueta–[301].

Específicamente, Mik critica incluso el ejemplo de Szabo de la *vending machine* como antepasado de los *Smart Contracts*, cuando en realidad sólo es una oferta para contratar, dirigida a público indeterminado, y la máquina en sí automatiza la formación y el cumplimiento del contrato cuando el co-contratante inserta una moneda. Pero lo mismo puede decirse hoy de todos los e-commerce, o de Amazon, o de cualquier caso de venta digital, como Spotify o Netflix. Así, sostiene Mik que el solo hecho de que la lógica de negocio se programe dentro de un software o hardware determinado no convierte *ipso facto* a dicho hardware o software en un contrato. Ni una máquina dispensadora ni un website son contratos, solo entregan bienes (o autorizan el acceso) en caso de haberse pagado por ello. Automatizar una transacción, o ciertas partes de la misma, no implica que exista un *contrato*, ni vuelve a la transacción *per se* inteligente[302].

Desde esta percepción crítica, se afirma vigorosamente que los contratos inteligentes no son ni contratos, ni son inteligentes, y que además no resuelven los verdaderos problemas de la vida real, por varias razones: (i) al ser un programa, deben ser escritos en alguno de los lenguajes que se usan, principalmente, *Solidity* para Ethereum[303]; (ii) la gente normal no entiende

ni conoce sobre lenguajes de programación y no puede verificar que el *script* efectivamente dice lo que tiene que decir; (iii) al desplegarse en una *blockchain*, estos programas –que no son contratos– no pueden frenarse ni revertirse, debido a la inmutabilidad de la *blockchain*; (iv) ningún software está libre del riesgo de errores de programación –*bugs*– y (v) muchos términos contractuales simplemente no pueden ser codificados en líneas de código [\[304\]](#).

Con una misma visión crítica, se ha sostenido que si bien es cierto que los actores con muchos recursos generalmente obtienen generalmente mejores resultados en Tribunales que los pequeños actores –generalmente más pobres [\[305\]](#)–, es harto discutible que los *Smart Contracts per se* tengan realmente tanto poder de transformación genuino, ya que los contratos inteligentes se enfocan demasiado en las medidas preventivas de seguridad, *ex ante*, y no tanto en las correctivas, *ex post*, y ello no resuelve todo el problema, del mismo modo que el cierre centralizado de puertas y las alarmas de un auto no vuelven innecesaria la necesidad de presencia y persecución policial cuando el robo del auto tiene lugar [\[306\]](#). En este sentido, críticamente se ha afirmado que los *Smart Contracts*, por su inherente limitación de ser un programa, no pueden capturar las complejidades sociales que rodean a la costumbre de contratar, y de hecho su inflexibilidad puede ser indeseada [\[307\]](#).

De otro costado, es interesante el enfoque de Rohr [\[308\]](#), quien se refiere a los contratos inteligentes como:

“a computer protocol (code) that is stored on a blockchain (or distributed ledger) and which will be automatically executed by the nodes on the blockchain’s network upon the occurrence of specified conditions. **Although they can be, Smart Contracts are not necessarily legal contracts.** Because of blockchain’s immutability, Smart Contracts that have been uploaded to the blockchain take on a life of their own: **they cannot be**

unilaterally stopped, delayed, or modified absent a fundamental change to the protocol of the blockchain on which the code resides or an “out” that was incorporated into the code from the outset ” (el resaltado es mío)

Es también interesante el enfoque de Arcari^[309], quien los define como programas representados por código electrónico, instalado y que corre en una *blockchain*, y que permite el intercambio de dinero, propiedades, acciones, u otro tipo de contraprestaciones entre las partes. Desde el punto de vista legal, Arcari sostiene que los contratos inteligentes son acuerdos automatizados, que hacen depender el cumplimiento del contrato sobre el acaecimiento o no de ciertas condiciones objetivas, predeterminadas en el código de programación de los mismos, de acuerdo a lo pactado en un contrato.

Ahora bien, se ha afirmado que los enamorados de los *Smart Contracts* se confunden al no reconocer las importantes diferencias legales entre *execution* y *enforcement*, que podríamos traducir como cumplimiento *voluntario* y cumplimiento *forzado* del contrato^[310]. Hoy por hoy miles de contratos se *cumplen voluntariamente*, de manera automatizada, especialmente en la industria financiera. Ahora bien, la novedad de los contratos inteligentes bajo estudio, es que las partes podrán “programar” el cumplimiento *forzado*, de modo tal que el co-contratante se desprende *ex ante* de su decisión de cumplir o no cumplir un contrato válidamente celebrado, y cede dicha facultad-deber-obligación a una *blockchain*. Y esto último, “automatizar el cumplimiento forzado”, es bastante distinto a “automatizar el cumplimiento voluntario”.

Por otro lado, con una visión menos crítica, se ha definido a los contratos inteligentes como el código de un programa de computación que automatiza la verificación, la ejecución y el cumplimiento de ciertos términos y condiciones de un contrato^[311]. También se los define como software autónomo, que permite que un registro distribuido funcione como una computadora distribuida, de modo tal que el mismo algoritmo de consenso que verifica que cada nodo tenga la misma copia del registro, le permite al

nodo realizar tareas idénticas computadas en un mismo orden ^[312].

Es también interesante la visión de Raskin ^[313], que por su parte los define como contratos cuya ejecución se ha automatizado mediante una o más computadoras, con la intención de asegurar su cumplimiento sin tener que recurrir a los Tribunales ante el incumplimiento, y por ende, eliminando la discrecionalidad humana respecto a su (in)cumplimiento. Estos contratos “controlan” el activo físico o digital que constituye su objeto y sobre los cuales se predica el cumplimiento contractual. Raskin propone diferenciar entre contratos inteligentes fuertes y débiles: (i) en los *fuertes*, el costo de revocar o modificar el *Smart Contract* es prohibitivo; y (ii) en los *segundos* –débiles– sucede lo contrario. Ergo, si un Tribunal puede modificar un *Smart Contract* luego de que ha sido cumplido con facilidad, entonces es un contrato inteligente débil, y no difieren en su esencia de un contrato convencional. Ahora bien, si el costo de modificar un contrato inteligente ya cumplido es muy alto, entonces estamos frente a un contrato inteligente *fuerte*, y esto si es novedoso para el Derecho.

La prestigiosa AMERICAN BAR ASSOCIATION también se ha ocupado de los contratos inteligentes en estos términos:

“Smart Contracting is a disruptive advancement that will have far-reaching impact for many industries, including financial services, government, real estate, manufacturing, and healthcare. For example, in securities trading, it currently takes several days to transfer assets, thereby increasing counterparty risk. Smart Contracts that use blockchain technology could shorten settlement times and mitigate such risk. In the insurance industry, certain policy agreements could be automated. A Smart Contract for travel insurance can be automatically triggered once a flight is cancelled. Once the cancellation is posted, the Smart Contract makes a payment directly to the policyholder, thereby bypassing the claims process. Governments may use Smart Contracts to manage title recordings, social services, and e-voting. In manufacturing,

Smart Contracts may replace current supply-chain processes such as bills of lading, proof of origin, or quality control. Another interesting application is tying Smart Contracts to the Internet of Things (i.e., cars, appliances, and devices). For example, a washing machine may contain a sensor indicating when it is low on detergent and then automatically reorder it (...) **as Smart Contract technology evolves, it will surely disrupt many industries (...)** It is only a matter of time before the technology is fully implemented. Lawyers can play an active role by staying abreast of changes that may affect their clients. Transactional lawyers may wish to learn more about the technical aspects of their future “Smart Contract” to ensure that it aligns with their client’s wishes and goals. In the future, litigation attorneys may no longer be litigating the “four-corners” of the contract, but rather expanding into the intent of the code.”^[314] (el resaltado es mío)

Desde un punto de vista más tecnológico, y menos legalista, Vitalik Buterin, creador de Ethereum, los define como:

“Cryptographic “boxes” that contain value and only unlock it if certain conditions are met^[315]”

Y también como:

“Ethereum is a decentralized platform that runs Smart Contracts: **applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.** These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in

accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk.”^[316] (el resaltado es mío)

Gideon Greenspan, también un referente en el ecosistema *Blockchain*, fundador de *MultiChain*^[317], define a los *Smart Contracts* como:

“...a piece of code that is stored on an blockchain, triggered by blockchain transactions and which reads and writes data in that blockchain’s database. That’s it. Really. A Smart Contract **is just a fancy name for code that runs on a blockchain**, and interacts with that blockchain’s state. And what is the code? It’s Pascal, it’s Python, it’s PHP. It’s Java, it’s Fortran, it’s C++. If we’re talking databases, it’s stored procedures written in an extension of SQL.”^[318] (el resaltado es mío)

A su turno, los prestigiosos –y muy citados– Profesores Wright y De Filippi^[319] los definen como:

“Digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention. In some cases, Smart Contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into source code. Contracting parties can thus structure their relationships more efficiently, in a self-executing manner and without the ambiguity of words. **Reliance on source code enables willing parties to model contractual performance and simulate the agreement’s performance before execution.** In other cases, Smart Contracts introduce new codified relationships that are both defined and automatically enforced

by code, but which are not linked to any underlying contractual rights or obligations. [\[320\]](#)”(el resaltado me pertenece)

Wright y De Filippi afirman también que los programadores creen que los *Smart Contracts* pueden facilitar la comunicación entre máquinas y la creación de organizaciones descentralizadas [\[321\]](#).

Por su parte, O’Shields [\[322\]](#) los define como:

“Smart Contracts are self-executing electronic instructions drafted in computer code. This allows a computer to “read” the contract and, in many cases, effectuate the instruction—hence the “smartness” of the contract. Smart Contracts self-execute the stipulations of an agreement when predetermined conditions are triggered. The parties “sign” the Smart Contract using cryptographic security and deploy it to a distributed ledger, or blockchain. When the conditions in the code are met, the program triggers the required action. Smart Contracts are a step beyond typical electronic contracts in that the actual agreement is embodied in computer code, rather than English or another traditional language.”

O’ Shields también aclara que variaciones de los *Smart Contracts*, tales como sistemas que procesan transacciones y efectúan pagos diarios computarizados entre entidades financieras, existen desde hace décadas [\[323\]](#).

Quizás con la máxima claridad posible, Clack, Bakshi y Braine [\[324\]](#) los definen como:

“A Smart Contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof

execution of computer code.”

En uno de los primeros trabajos que abordó la temática de los *Smart Contracts* desde la óptica de los Abogados, Samuel Bourque y Sara Fung Ling Tsui los conceptualizaron del siguiente modo:

“Simply put, a Smart Contract is a self-executing contract. To wit, SCs are just like traditional paper contracts drafted in natural human language only that SCs specifically are drafted electronically in a computer interpretable language. The important effect is that the computer system that interprets the SC can execute some of the terms of the contract.”^[325]

Koulu^[326], por su parte, los define como:

“A Smart Contract is an automated software program built on a blockchain protocol; basically Smart Contracts are made possible by general-purpose computation that takes place “on” the blockchain. They can be used for allocating digital currency between two parties, when the requirements established in the program/contract are fulfilled. In short, Smart Contracts are **programmable contractual tools, they are contracts embedded in software code**. Thus, a Smart Contract can include the contractual arrangement itself, governance of the preconditions necessary for the contractual obligations to take place and the actual execution of the contract. To say that Smart Contracts are self-enforceable means that the software executes the contract, e.g. **allocates digital assets autonomously and regardless of trust between the parties**. Receiving a payment for sold goods is then no longer dependent on the willingness of the debtor to make the payment nor affected by bankruptcy proceedings that take place after entering the contract. The contract executes its

content autonomously according to the embedded contract terms e.g. the digital assets placed within the contract are allocated by the software and no external monitoring of contractual obligations or enforcement is needed.” (El resaltado es mío)

Otra definición conceptualiza a los *Smart Contracts* como código de computación auto-ejecutable que procesa automáticamente sus *inputs* cuando son activados, cuya propuesta de valor es su cumplimiento automático [\[327\]](#). Se trata de aplicaciones de segundo nivel que corren en la *blockchain*, y al igual que ésta, una vez desplegados no pueden ser modificados, salvo que hayan sido programados con tal característica.

Kaal y Calcaterra, a su turno, definen y ejemplifican los *Smart Contracts* del siguiente modo [\[328\]](#):

“Smart Contracts and smart property are blockchain enabled computer protocols that verify, facilitate, monitor, and enforce the negotiation and performance of a contract. An often-cited example for Smart Contracts is the purchase of music through Apple’s iTunes platform. A computer code ensures that the “purchaser” can only listen to the music file on a limited number of Apple devices.”

A nivel institucional, hay conceptualizaciones muy pertinentes. Por caso, la prestigiosa CHAMBER OF DIGITAL COMMERCE de EE.UU [\[329\]](#) define a los *Smart Contracts* como “un código de computadora que, dado el acaecimiento de una o unas condiciones especificadas, es capaz de auto-ejecutarse automáticamente según una serie de funciones predeterminadas. El código se puede almacenar y ejecutar en un registro distribuido y puede dejar registrado en éste cualquier cambio resultante”. Se afirma también que un *Smart Contract* no es necesariamente un contrato en el sentido legal, sino más bien una forma avanzada de instrucciones condicionales del tipo “Si ocurre X, entonces Y” escrito en código de computadoras.

La Universidad de Yeshiva, por su parte, cuenta con un muy interesante y prestigioso proyecto dedicado al estudio de la *blockchain*, llamado CARDOZO *BLOCKCHAIN* PROJECT, que también ha definido a los *Smart Contracts*:

“Because blockchains store tamper resilient, transparent, and non-repudiable data, the technology is being used for far more than just maintaining records of digital currency transactions. Indeed, blockchains are storing or referencing, other forms of information; blockchain-based protocols are layering additional technology to process what can essentially be thought of as small computer programs—what technologists often refer to as “Smart Contracts”(…) are being used to memorialize a portion of a parties’ agreement, with a **Smart Contract assisting with one or more performance obligations and traditional legal prose memorializing other basic contractual rights, obligations, and conditions**—such as representations and warranties and choice of law and dispute resolution provisions. These “hybrid” agreements blend together traditional legal prose—written in a natural language like English—with Smart Contract programs written in code. **The written agreement references and incorporates a Smart Contract and contextualizes how the program fits into a larger contractual arrangement.** ^[330]” (el resaltado es mío)

En Europa, por otra parte, el flamante OBSERVATORIO Y FORO DE *BLOCKCHAIN* DE LA UNIÓN EUROPEA también se ha ocupado de los *Smart Contracts*, y los ha definido, en el contexto de *blockchain*, como código de computación que está almacenado en una cadena de bloques y que puede ser accedido por una o mas partes ^[331]. Se afirma que los *Smart Contracts* no son generalmente contratos en un sentido legal, y que pueden ser usados para cosas muy interesantes, como tokenizaciones; para codificar y automatizar procesos de negocio que puedan ser compartidos entre múltiples partes, generando reducción de costos y ganancias de eficiencias; o para codificar

contratos entre partes en relación a la transferencia de valor o determinados activos –tales como *escrow agreements*, o contratos con cláusula de pago contra entrega–, de un modo transparente, y con ejecución automática basada en determinadas condiciones, dificultando o imposibilitando el incumplimiento de la contraparte [\[332\]](#).

Finalmente, en Argentina, Santiago Mora los ha definido como un contrato electrónico con la característica distintiva de que él mismo hace cumplir sus propios términos, por lo que habitualmente estará lleno de instrucciones y condiciones propias del código informático que siguen un patrón típico de “si esto ocurre, haz esto; pero si no ocurre, haz esto otro”, y una vez iniciada la ejecución, las partes dejan de tener control sobre su cumplimiento [\[333\]](#). Otra definición es la dada por Mirassou Canseco y Hadad, que los definen como como programas informáticos que facilitan, aseguran, hacen cumplir y ejecutan acuerdos registrados entre dos o más partes (personas físicas o jurídicas). Son algoritmos que operan con la característica principal de no poder ser controlados por ninguna de las partes y de ser autoejecutables, es decir, su ejecución se encuentra automatizada [\[334\]](#).

A continuación, una imagen de cómo “se ve” un *Smart Contract*:

Imagen 9: *Smart Contract* Town Crier

Town Crier blockchain contract C_{TC} with fees

Initialize: Counter := 0

Request: On recv (params, callback, $\$f$, $\$g_{req}$) from some C_U :

Assert $\$G_{min} \leq \$f \leq \$G_{max}$
id := Counter; Counter := Counter + 1
Store (id, params, callback, $\$f$, C_U) // *msg.m₁*
// $\$f$ held by contract

Deliver: On recv (id, params, data, $\$g_{dvr}$) from W_{TC} :

- (1) If isCanceled[id] and not isDelivered[id]
Set isDelivered[id]
- (2) Send $\$G_0$ to W_{TC}
Return
Retrieve stored (id, params', callback, $\$f$, -)
// *abort if not found*
Assert params = params' and $\$f \leq \g_{dvr}
and isDelivered[id] not set
Set isDelivered[id]
- (3) Send $\$f$ to W_{TC}
Set $\$g_{clbk} := \$f - \$G_{min}$
- (4) Call callback(data) with gas $\$g_{clbk}$ // *msg.m₄*

Cancel: On recv (id, $\$g_{cncl}$) from C_U :

Retrieve stored (id, -, -, $\$f$, C'_U)
// *abort if not found*
Assert $C_U = C'_U$ and $\$f \geq \G_0
and isDelivered[id] not set
and isCanceled[id] not set
Set isCanceled[id]

- (5) Send $(\$f - \$G_0)$ to C_U // *hold $\$G_0$*

Imagen 10: Smart Contract Buterin

```

init:
    contract.storage[0] = msg.data[0] # Limited account
    contract.storage[1] = msg.data[1] # Unlimited account
    contract.storage[2] = block.timestamp # Time last accessed
code:
    if msg.sender == contract.storage[0]:
        last_accessed = contract.storage[2]
        balance_avail = contract.storage[3]

        # Withdrawal limit is 1 finney per second, maximum 10000 ether
        balance_avail += 10^15 * (block.timestamp - last_accessed)
        if balance_avail > 10^22:
            balance_avail = 10^22

        if msg.data[1] <= balance_avail:
            send(msg.data[0], msg.data[1])
            contract.storage[3] = balance_avail - msg.data[1]
            contract.storage[2] = block.timestamp

    # Unlimited account has no restrictions
    elif msg.sender == contract.storage[1]:
        send(msg.data[0], msg.data[1])

```

2.1.1. Clasificación de los contratos inteligentes

Se presentan, a los fines didácticos de este Manual, tres clasificaciones. Una es la que nos da el OBSERVATORIO Y FORO DE *BLOCKCHAIN* DE LA UNIÓN EUROPEA, que propone analizar esta nueva realidad “contractual” dividiéndola en dos: (i) *Smart Legal Contracts*: que son contratos inteligentes en una cadena de bloques que representan o emulan un contrato en el sentido legal del término; y (ii) *Smart Contracts con Implicancias Legales*: construcciones o artefactos basados en nuevas tecnologías que claramente tienen implicancias legales [\[335\]](#).

Los *Smart Legal Contracts* implican que, en una legislación dada, éstos contratos son legalmente válidos por cumplir los requisitos que se exigen a cualquier contrato [\[336\]](#). Puntualmente respecto a la forma escrita de los contratos, la cuestión que se presenta es si el lenguaje computable –que no es lenguaje natural– puede ser considerado un lenguaje apto para configurar la

creación de derechos y obligaciones, teniendo en cuenta que los contratos *formales* son sólo aquéllos a los cuales la ley les impone una forma determinada [\[337\]](#). Por otro lado, en caso que el contrato inteligente haya sido celebrado por adhesión, incluyendo por medios electrónicos o similares [\[338\]](#), la parte predisponente debe redactar el contrato de modo claro, completo y fácilmente legible [\[339\]](#), y se tienen por no escritas las cláusulas que por su redacción o presentación, no son razonablemente previsibles [\[340\]](#). ¿El lenguaje computable –una instrucción– es fácilmente legible? ¿Su forma de redacción permite razonablemente prever el efecto que producirá?

Por otro lado, señala el OBSERVATORIO Y FORO DE *BLOCKCHAIN* DE LA UNIÓN EUROPEA que los *Smart Contracts* con Implicancias Legales son aquellos programados para: (i) representar activos de forma digital [\[341\]](#); (ii) crear DAOs [\[342\]](#); y/o (iii) actuar como agentes descentralizados [\[343\]](#) (se volverá sobre las DAOs más abajo en § 2.6).

Otro criterio de clasificación interesante es el propuesto por Samuel Bourque y Sara Fung Ling Tsui, que los divide entre contratos inteligentes *suaves o puros*, dependiendo de: (i) el nivel de automatización de la ejecución contractual [\[344\]](#); (ii) el grado de separación que exista entre los términos acordados en el contrato convencional subyacente y los términos codificados en algún lenguaje computable [\[345\]](#); y (iii) dónde reside el código del contrato inteligente, y su grado de “discreción” para ejecutar la instrucción, sin interferencia de las partes [\[346\]](#).

En los *Smart Contracts puros*, el propio código programado es el contrato, y esto solo ha sido posible con el surgimiento de Bitcoin y la *blockchain*, ya que el contrato ahora efectivamente puede controlar criptomonedas. Por todo ello, sostienen los autores citados que las características esenciales de los *Smart Contracts puros* son: (a) mayor transparencia sobre los términos contractuales y su ejecución; (b) la separación entre la ejecución del contrato y la voluntad de las partes; y (c) la automatización de las obligaciones del

contrato.

Finalmente, un tercer criterio [\[347\]](#) de clasificación de contratos inteligentes, los divide en:

1) *Contrato inteligente en sentido operacional*: se refiere a software que normalmente es utilizado en DLTs. La palabra *contrato* hace referencia a que este software cumple obligaciones o ejerce derechos, pudiendo para ello controlar ciertos activos dentro del DLT; y

2) *Contrato inteligente en sentido legal*: se refiere a cómo un contrato convencional puede ser expresado y ejecutado mediante uso de software. Aquí se vinculan aspectos operacionales, pero también aspectos vinculados a cómo se escriben los contratos convencionales, y cómo deben interpretarse. En esta clasificación se inscriben desarrollos como la integración dual [\[348\]](#) y los contratos Ricardianos [\[349\]](#), que se verán más abajo.

2.1.2. Naturaleza jurídica de los contratos inteligentes

Las teorías sobre la naturaleza jurídica de un contrato inteligente incluyen las siguientes posturas: (i) es un fideicomiso [\[350\]](#); (ii) es un representante de las partes [\[351\]](#); o (iii) es una persona jurídica –véase más abajo, en § 2.6– [\[352\]](#); o (iv) es un contrato en sentido legal convencional.

Específicamente con relación a la *blockchain*, los *Smart Contracts* y los *trusts* del common law, se ha sostenido [\[353\]](#) que pueden constituirse fideicomisos *on-chain* que operen mediante *Smart Contracts*. En efecto, la AMERICAN BAR ASSOCIATION propone:

“DL technology and Smart Contracts have the **potential to be used in trust creation and estate administration**. The division

of assets in an estate could potentially be cryptographically and securely coded into the blockchain which, upon the passing of the testator and the registration of the death certificate, **the terms of the will or trust could self-execute to disburse the assets**. The piloted service Blockchain Apparatus advertises the potential to administer and execute will documents without human involvement, even allowing for revisions of the documents, which are stored in their own original state, to preserve the right to amend. Although blockchain is unable to remove all the legal disputes around the creation of a will, such as issues regarding ambiguous terms and claims that the testator was under duress, it has the potential to streamline and expedite the estate administration process and ‘make it much easier for a genuine will to be upheld, for a bogus challenge to be dismissed, and for courts to come to factual findings much more quickly’. The need for wills and estate lawyers will likely endure, as they are required to draft and encode these legal documents. However, the digitisation of the industry and the increasing use of pre-drafted will templates may put pressure on these practitioners to become technologically literate in order to remain relevant and competitive.” (el resaltado es mío)

Siguiendo el criterio del OBSERVATORIO Y FORO DE *BLOCKCHAIN* DE LA UNIÓN EUROPEA antes expuesto, puede afirmarse que la naturaleza jurídica de los contratos inteligentes permite diferenciar entre los *Smart Legal Contracts*, que son (o pueden ser) contratos, según la definición legal de cada legislación implicada, y, pueden (o no) ser legalmente válidos como cualquier contrato si cumplen los requisitos que se les exigen a todos los contratos.

Pero, como se verá más abajo, existen otros *Smart Contracts con Implicancias Legales*, que son aquellos programados para representar activos de forma digital, o crear DAOs, o actuar como agentes descentralizados.

La naturaleza jurídica de estos contratos inteligentes *con Implicancias Legales* puede ampliamente exceder la calificación de un *mero* contrato, para asumir o combinarse con otras formas jurídicas mucho más complejas, como contratos multilaterales de organización que en un futuro próximo podrán (o

no) ser personificados por la ley, con capacidad para, de modo autónomo o con alguna supervisión humana, ejercer derechos, contraer obligaciones y actuar en beneficio de sus representados en un entorno digital y *on-chain*.

2.1.3. *Contratos inteligentes y el ejercicio de la profesión de Abogado*

¿Se requiere el asesoramiento profesional de un Abogado para negociar un contrato inteligente? ¿Es conveniente? ¿Es necesario? ¿Es posible?

Bourque y Tsui se pronuncian, sin hesitar, por la afirmativa y sostienen que el ejercicio de la profesión de abogado debe ser ampliado para incluir, por mandato legal, el asesoramiento en la redacción de contratos inteligentes [\[354\]](#).

2.1.4. *Smart Contracts vs. Computable Contracts*

En 2012, Harry Surden, profesor de Derecho en las Universidades de Stanford y Colorado publicó un muy célebre artículo, al que tituló *Computable Contracts* [\[355\]](#), en el que analizaba cómo y para qué las empresas “codifican” ciertas obligaciones contractuales como datos computables. Describió y rotuló tal práctica como *contratación orientada a datos*, muy utilizada en contratos financieros –e.g. contratos de opción sobre acciones– que se representan como registros de datos con una finalidad expresa de ser luego procesados por computadoras –recordar la definición de Buterin sobre *Smart Contracts*.

La claridad envidiable de Surden justifica detenernos a analizar en profundidad sus ideas.

2.1.4.1. *Términos contractuales computables*

Las empresas saben (o debieran saber) que administrar contratos es un proceso costoso, que requiere mucho talento humano. Contratar es un

proceso compuesto de varios (costosos) pasos: determinación de cuál contrato utilizar, negociarlo, firmarlo, monitorear su cumplimiento, analizar su impacto en materia de precios y suministros, e integrar toda esa información en unidades funcionales como la cadena de suministros, y convertirlo en insumo informativo para la toma de decisiones [\[356\]](#).

Especialmente los contratos comerciales, involucran obligaciones de acuerdo a términos y condiciones pactados, cuyo cumplimiento es (o debiera ser) supervisado de manera continua. Supervisión ésta que cuesta dinero. Y, lógicamente, mientras más grande la red contractual de una empresa, más costoso verificar su cumplimiento, mayores *costos de transacción*. Para abaratar tal centro de costos, se recurre cada vez más a la tecnología.

Ahora bien, sin traer a colación los (hiper) importantes desarrollos en materia de Inteligencia Artificial aplicada al lenguaje natural y a la administración contractual que han tenido lugar entre 2012 y 2020 [\[357\]](#), Surden señalaba en 2012 que muchos afirmaban que la tecnología *no podía aún* automatizar la supervisión y el *compliance* contractual, entendido éste proceso como un *iter* de dos tramos: (i) *entender* qué se pactó [\[358\]](#) y bajo qué condiciones y luego (ii) comparar lo que se pactó con lo que ocurrió (o no) finalmente [\[359\]](#). Tal afirmación del año 2012 se justificaba, por un lado, en las (grandes) limitaciones para entender el lenguaje humano y natural por parte de los algoritmos (que existían en 2012) [\[360\]](#). Por otro lado, para analizar el *cumplimiento contractual*, comparando los hechos ocurridos contra las palabras preexistentes, deben superarse otras limitaciones. En efecto, los contratos frecuentemente contienen términos de textura abierta, para tener cierta flexibilidad de cara a acontecimientos futuros e inciertos [\[361\]](#). Las personas reaccionan de un modo *humano* ante términos adrede *abiertos*, que las computadoras pueden no entender, ya que son complejos procesos cognitivos y, de nuevo, humanos.

No obstante dichas dificultades, Surden afirmaba que ciertas obligaciones contractuales se pueden representar en un lenguaje que no es lenguaje natural, sino un lenguaje que las máquinas pueden procesar y entender. *Machine-readable, computer data*. Este enfoque de Surden propone y afirma

el auge de los *contracts-as-data* ^[362], y señala que se emplean mucho en el mundo de las finanzas, e.g. contratos derivados sobre moneda extranjera, para que puedan ser procesados por sistemas electrónicos de *financial trading*. En estos casos, tanto las obligaciones contractuales como la información necesaria para cumplir la obligación está disponible en *machine-readable format*, con lo cual un software puede comparar lo prometido vs. lo ocurrido.

Así, los contratos que permiten esa puntual mejora tecnológica, son los *Computable Contracts* de Surden, quien los denomina también como *data-oriented contracts*, aquellos en los que las partes han expresado una porción ^[363] de sus términos y condiciones como datos procesables por una computadora, para que ésta pueda controlar su cumplimiento posterior. Evidentemente, el concepto es muy similar al de *Smart Contracts* según se vio más arriba, pero no tiene en cuenta el complemento de la cadena de bloques ^[364].

2.1.4.2. Limitaciones de los *data-oriented contracts*

Poder expresar términos contractuales como datos computables abre un campo nuevo para las habilidades contractuales de los Abogados.

En efecto, los *data-oriented contracts* no se expresan igual que los contratos convencionales: aquéllos tienen términos y condiciones expresados como registros de datos estructurados, y éstos los expresan con lenguaje escrito y natural. Sin embargo, en los *data-oriented contracts*, no toda cláusula es computable, pero *algunas* cláusulas han sido pensadas para ser “leídas” por computadoras ^[365], lo que los diferencia, a su vez, de los contratos electrónicos, que no tienen éste tipo de cláusulas, y solo son un medio digital para expresar el lenguaje natural o humano ^[366].

Ahora bien, traducir ciertos términos legales a *machine-readable format* en forma de instrucciones de computación requiere estructurar los datos de un modo que, ciertamente, no admite que *todo tipo* de cláusulas se “traduzca” al lenguaje de la máquina, que es un lenguaje matemático ^[367]. Pero los

contratos pueden ser diseñados *ab initio* con esta intención, con un enfoque orientado a datos, donde las “opciones lingüísticas” son menores que las existentes en el lenguaje natural, y están pensadas para ser entendidas por una computadora.

Pero no sólo hay que traducir cláusulas en datos legibles para el lenguaje de la máquina, sino que hay que darles un sentido a esos datos, para que la máquina *entienda* qué significan [\[368\]](#) y ejecute la instrucción que corresponda. Las partes contratantes recurren para ello a (i) *data-meaning agreements* [\[369\]](#), a (ii) estándares generalmente aceptados sobre el significado de ciertos datos, muy frecuentes y comunes en el ámbito de las finanzas [\[370\]](#) y (iii) a *procedural agreements* que disponen cómo convertir expresiones contractuales en *data-oriented expressions* [\[371\]](#).

2.1.4.3. Otras limitaciones y beneficios

Los contratos que requieran un cierto grado de abstracción conceptual, o grados amplios de flexibilidad *ex post facto* para analizar hechos –o sus impactos–, o estén sujetos a determinaciones de profesionales expertos, o tengan intrínsecamente un alto grado de incertidumbre, no serán fácilmente computables [\[372\]](#). Sin embargo, en los casos en que sí sea posible computar contratos, los beneficios serán una reducción de los costos de transacción [\[373\]](#) y, en mayor medida, la contratación *machine-to-machine* [\[374\]](#).

2.1.5. La visión de Samuel Bourque

Así como el trabajo de Surden en 2012 ha sido sin dudas pionero, lo mismo puede decirse sobre Samuel Bourque, que comenzó a analizar los contratos inteligentes en 2014. Bourque se preguntaba en aquél momento si era necesario ser Abogado para asesorar en materia de contratos inteligentes, o si un contrato inteligente puede ser considerado una persona en sentido legal, o

si es necesario regularlos. Interesantes preguntas que comienzan a tener respuesta (parcial) recién en 2020. Por ello, nos detendremos en analizar la visión de este programador y abogado que vive en Hong Kong.

Bourque ha afirmado que el Derecho no ha visto muchos cambios tecnológicos, y que en general, los sistemas legales no compiten entre sí, salvo en materia de arbitraje institucional y de *forum shopping*. Por otro lado, ha señalado acertadamente que desde y gracias al surgimiento de Internet, la tecnología ha evolucionado encapsulada, un poco al margen del Derecho, porque los programadores normalmente *ignoran* el Derecho.

Con relación a los *Smart Contracts*, Bourque señala que no son un concepto nuevo, pero al asociarse y vincularse con criptomonedas, comienzan a desarrollarse sin tener que recurrir a los bancos, que nunca serían partes de *Smart Contracts* programados por particulares.

Según Bourque, los *Smart Contracts* son *una nueva plataforma para el desarrollo de aplicaciones para transacciones complejas* ^[375]. Los clasifica en (i) suaves (Amazon, Apple, mercados de futuros): son contratos tipo *take it or leave it*, donde una parte –e.g. Amazon– ejecuta todas las obligaciones e incluye referencias a T&Cs contenidos en otros lugares, que pueden modificarse sin que se modifique el contrato inteligente suave, que sólo ejecuta una parte de las obligaciones que está programada para ser automatizada; o (ii) puros: que son la segunda generación de contratos inteligentes que la *blockchain 2.0* permite.

Bourque aclara, con razón, que un *Smart Contract* no es necesariamente un contrato en sentido legal. Un *Smart Contract* es una plataforma de desarrollo, y lo desarrollado en ella puede no cumplir con los requisitos de un contrato. Un *Smart Contract* es más bien una instrucción, o una serie de instrucciones condicionales, escritas en el lenguaje de programación en una plataforma que permite ejecutar las instrucciones. Precisa, además, que con relación al cumplimiento contractual, todo lo que puede ser hecho on line, puede ser “tercerizado” a un *Smart Contract*. Y con el desarrollo de la IoT y la *Smart Property*, se pueden vincular con el mundo *off-line*.

Sostiene Bourque que hay muchos beneficios por desarrollar *Smart Contracts* puros:

- i) menos ambigüedad, por la necesidad del lenguaje de programación;
- ii) más claridad en sus términos, ya que el contrato es el código y el código es el contrato;
- iii) pre-verificable: el compilador detecta si hay un error de sintaxis, con lo cual se puede chequear el contrato antes de iniciarlo;
- iv) predecible: se puede simular y se puede testear fuera del mundo real;
- v) eficiencia: permite automatizar procesos;
- vi) privacidad: se puede encriptar;
- vii) más barato: usar el sistema de justicia convencional para reclamar incumplimientos contractuales es caro, pero desarrollar un *Smart Contract* tampoco es gratis; y
- viii) independencia: Amazon puede tener un conflicto de interés en inclinar los T&Cs a su favor; en cambio en los *Smart Contracts*, hay una plataforma, quizás Ethereum, que cumple los términos del contrato, así como su ejecución, de manera imparcial y agnóstica.

Señala que también hay importantes problemas vinculados a los *Smart Contracts*:

- i) cuestiones de lenguaje: poca gente puede leer el lenguaje de programación;
- ii) sofisticado: no es sólo el lenguaje, sino también la forma de pensar, orientada a los detalles; programar requiere mucho detalle y entendimiento;
- iii) tedioso;
- iv) la infraestructura tecnológica: no todo está digitalizado y eso puede frenar el desarrollo de los contratos inteligentes;

v) resistencia de sistemas precedentes –*legacy systems*–: habrá que modificar leyes para que algunas transacciones sean 100% digitalizadas;

vi) vinculación tecnológica: ejemplifica el autor citado que si quieres escribir un *Smart Contract* sobre una stock option, tenés que recurrir a información de terceros, y si esta información es incorrecta, el contrato no funcionará bien.

Señala Bourque los siguientes atributos de los contratos inteligentes:

Privacidad: esta es una característica esencial. Se pueden encriptar, *hashear*, y es fácil darles privacidad. Además, hay una sola versión del contrato, alojada en la plataforma de que se trate.

Firmas: con la tecnología de *Public Key Infrastructure* (PKI), hay una llave pública y una privada, y si las juntas podés identificar a la persona. La identidad PKI puede ser uni-direccional o bi-direccional. Uni-direccional: desde el contrato *per se*, no se puede saber quién es la parte contratante, salvo que se dé a conocer, aparezca y utilice la llave privada correspondiente. Bi-direccional: la parte es identificable y verificable. Cada contrato puede ser programado uni o bi-direccional.

Custodia: un *Smart Contract* tiene su propia *identidad*, su propia billetera (llave pública), su propia firma, o puede estar sujeto a múltiples firmas de terceros –es lo más parecido a una cuenta corriente que gira a la orden conjunta de dos o más partes– para operar o ejecutar acciones o disponer de activos digitales, y puede tener acceso a determinados derechos o a activos digitales. Quien ejecuta el contrato es la plataforma donde está programado, i.e. Ethereum, que es como si fuera un tercero invisible que es parte del contrato.

Cláusulas *off-line*: hay cláusulas de un contrato convencional que no son derechos ni obligaciones, por ejemplo: preámbulo, antecedentes, ley aplicable, forma de resolución de conflictos, cláusulas de *non-disclosure* o *non-competition*. Pero la resolución de conflictos se puede programar *dentro* del contrato, para que, por ejemplo, congele los fondos hasta tanto la disputa sea resuelta, o un árbitro decida quién tiene razón.

Pseudo-anonimidad: la *identidad* en *blockchain* es la *llave pública*, pero

nadie sabe a quién corresponde. Sin embargo, el caso *Silk Road* ejemplifica que es posible vincular la llave pública con una persona concreta si se quiere hacerlo.

En cuanto al funcionamiento de un contrato inteligente *per se*, Bourque lo asimilaba al de un web service: permite escuchar eventos (vía Oráculos), verificar si una parte tiene derecho a disponer determinados activos (*on-chain* y *off-chain*), ejecutar acciones según se requiera, automatizarlas, responder a preguntas de las partes, ser revisado, modificado, terminado, o borrado, si las partes acuerdan tal flexibilidad futura al momento de programarlo.

Señala Bourque que lo nuevo y disruptivo es que se combinan, por un lado, el contrato, sus términos y, por otro, la ejecución del contrato, en un único lenguaje, y la ejecución, a su vez, depende o se confía a una tercera parte: la *blockchain* donde corre. Además, los términos del código, o del contrato, son transparentes, están a la vista de todos.

Ya en 2014 Bourque también adelantaba conceptos sobre DAOs y DACs, que se analizan más abajo. Las definía como organizaciones donde el gobierno interno está automatizado por muchos contratos inteligentes. Es el *Corporate Governance 2.0*. Es una red de contratos, que puede ser programada para que sea autónoma. Pueden ser o no registradas en una jurisdicción determinada, o en una jurisdicción amigable. Pero no está implícito que deban estar registradas. Pueden emular el funcionamiento societario, o no [\[376\]](#).

2.2. Cuatro pilares fundamentales de los Smart Contracts

Siguiendo a Szabo, y dejando atrás la (fundada) polémica existente en punto a la naturaleza y utilidad actual o futura de los contratos inteligentes, se pueden apreciar y analíticamente separar cuatro pilares fundamentales que rodean o enmarcan la realidad de los contratos inteligentes.

2.2.1. Observabilidad: el regreso de la Pitonisa (reloaded) y los Oráculos

El término *observabilidad* hace referencia a la aptitud de las partes de un

contrato inteligente –o de un tercero por ellas designado– de poder observar recíprocamente el cumplimiento de la prestación a su cargo, i.e. de poder verificar que el cumplimiento de la prestación se ajusta a los términos pactados [\[377\]](#). Para facilitar este proceso de observación, es que aparece entonces el concepto de los *Oráculos*.

Los Oráculos pueden definirse como un programa de computación que opera de manera separada al código de un *Smart Contract*, y que recopila o tiene acceso a información *off-chain*, es decir, que no se encuentra en la *blockchain*, y la ponen a disposición del *Smart Contract*, para confirmar si las partes han cumplido lo pactado, o no [\[378\]](#). Evidentemente, el rol de los Oráculos es clave, puesto que si la información que entregan no es correcta o fidedigna, el *Smart Contract* no funcionará del modo que la intención común de las partes lo quiso.

Los Oráculos deben ser *per se* confiables. Así, existen *data feeds* que son, en sí mismos, *Smart Contracts* que interactúan con otros *Smart Contracts*, proveyendo simplemente información determinada [\[379\]](#). En este sentido, se ha sostenido que el Oráculo en alguna medida *empuja* la información externa hacia dentro de la *blockchain* –en lugar de un *Smart Contract* tirando la información hacia adentro de la *blockchain* [\[380\]](#)– y, obviamente, se asume que serán *muy* confiables, pero al ser un recurso que está captando datos de *afuera* de la *blockchain*, se afecta el carácter descentralizado de la cadena.

Mik define a los Oráculos como entidades que cuentan con la infraestructura técnica necesaria para comunicar a los *Smart Contracts* cierta información que refiere a hechos ocurridos afuera de la *blockchain* [\[381\]](#). Enseña Mik que los Oráculos no “insertan” la información de manera directa en la *blockchain*, sino que “firman”, con su llave privada, un *Smart Contract* que produce que un token –objeto del *Smart Contract*– se transfiera con algún destino preestablecido, si un hecho externo *off-chain* X efectivamente ocurrió. Subraya también las grandes dificultades que existen en la materia: (i) es difícil conseguir Oráculos confiables [\[382\]](#), (ii) es difícil conseguir fuentes externas fiables de datos, (iii) los dos aspectos anteriores ponen en

duda la propia seguridad ofrecida por una *blockchain*, al recurrir a elementos *off-chain* que no gozan de los atributos de seguridad de una *blockchain*, y (iv) muchos hechos externos a la cadena de bloques no pueden representarse en *machine-readable format* [\[383\]](#).

Buterin [\[384\]](#), por su parte, describe el funcionamiento de los Oráculos del siguiente modo:

“Essentially, instead of a long-running contract being run directly on the blockchain, all funds that are intended to go into the contract would instead go into an **M-of-N multisig address controlled by a set of specialized entities called “oracles”, and the contract code would be simultaneously sent to all of these entities**. Every time someone wants to send a message to the contract, they would send the message to the oracles. The oracles would run the code, and if the code execution leads to a withdrawal from the contract to some particular address then the oracles circulate a transaction sending the funds and sign it.” (el resaltado es mío)

Werbach, finalmente, afirma:

“**Oracles can also be humans**. Consider a simple Smart Contract in which each of the parties has a private key and a third key is given to an expert arbitrator. The Smart Contract requires two of three keys in order to execute. If the parties agree the contract has been fully performed, they each provide their key and the Smart Contract executes. If there is a dispute, they turn to the arbitrator. She either provides her key along with that of the party seeking to enforce the contract or refuses it and therefore prevents completion of the transaction. This system mimics a legal arbitration process.” (el resaltado me pertenece)

Para finalizar, se trae a colación un caso muy interesante de diseño de un Oráculo implementado por SWIFT [\[385\]](#) recientemente [\[386\]](#), con el objetivo de proveer de información *off-chain* a los *Smart Contracts* de varias redes, que permitirán hacer pagos y liberar garantías en más de 11.000 bancos que forman parte de SWIFT [\[387\]](#).

2.2.2. Verificabilidad

La verificabilidad implica la posibilidad real de cualquiera de las partes involucradas en un *Smart Contract* –o de un tercero árbitro, en su caso– de poder demostrar ante un tercero (o que éste pueda corroborar) que el contrato se cumplió, o que no se cumplió [\[388\]](#).

Este atributo, según Szabo, es muy propio de los contratos inteligentes ya que es necesario que un tercero verifique el cumplimiento (o su falta); algo que en los contratos convencionales es determinado sólo por las partes. Igualmente, es quizás el elemento más complejo de los contratos inteligentes, ya que también se vincula con la prueba de identidad de las partes *on-chain*, ya que el árbitro debe conocer la identidad de las partes para poder resolver conflictos eventuales.

Siguiendo a Arcari en este punto [\[389\]](#), la verificabilidad tiene dos aspectos: (i) acceso abierto a la información para el árbitro; y (ii) que las partes cumplan con la obligación de proveer esa información al árbitro –o que acuerden qué Oráculo será utilizado, si es que existe uno que sea adecuado según la naturaleza del *Smart Contract*. La presencia de este árbitro implica el nacimiento de una nueva e interesante rama del Derecho, y ya comienzan a ofrecerse estos servicios por parte de estudios jurídicos en todo el mundo [\[390\]](#), recomendándose la utilidad de diseñar en cada contrato inteligente una cláusula de verificabilidad, similar a una cláusula de resolución de controversias en un contrato convencional. El arbitrador suele ser un abogado, y se afirma que:

“Smart Contract arbitration still **offers efficiency** for Smart Contract parties despite the human influence, **particularly its speed and flexibility**. Arbitration often takes a fraction of the time a court case and additionally arbitration’s flexibility provides a neutral venue to enable parties to efficiently resolve disputes, wherever they are located.”^[391]

Finalmente, Arcari afirma que un árbitro necesita dos tipos de información para resolver: (i) información referida a datos que están fuera de la *blockchain* –quizás mediante Oráculos– y (ii) una versión del contrato inteligente en lenguaje natural, de modo tal que pueda entender cuál fue la intención de las partes al codificarlo^[392]. Según la materia sobre la cual verse el código del *Smart Contract*, puede que no existan Oráculos disponibles, y que la información pertinente deba entonces ser provista por las partes del contrato al árbitro, lo que debe estar previsto en el contrato por el cual se acordó automatizar ciertas partes de la relación contractual mediante su codificación.

2.2.3. Privacidad (efecto relativo 2.0 +/- identidad +/- confidencialidad +/- anonimidad)

En el ámbito de los contratos inteligentes, la privacidad implica que sólo las partes contratantes (i) controlan, (ii) conocen y (iii) se benefician por la ejecución del contrato en una *blockchain*. La tercer característica antes mencionada, es una característica que comparten los contratos inteligentes con todos los contratos convencionales, y que se sintetiza en el conocido adagio latino, norma general del derecho de los contratos: *res inter alios acta, aliis nec prodesse, nec nocere potest*, también conocido como el principio del efecto relativo de los contratos^[393].

Ahora bien, evidentemente, las otras dos notas características de privacidad en los *Smart Contracts* tienen que ser precisadas, ya que se vinculan intrínsecamente con el control y con la confidencialidad, y también con las particulares formas de identidad –anonimidad y pseudonimidad– que la *blockchain* permite.

En *blockchain*, la privacidad se consigue de tres modos ^[394]: (i) operando anónimamente, utilizando por ejemplo tecnologías de *Zero Knowledge Proof* (ZKPs ^[395]); (ii) encriptando la información; y (iii) no alojando información sensible en una *blockchain*, sino en canales paralelos *off-chain* ^[396].

Seguidamente se presentarán los aspectos vinculados al *control de privacidad* del contrato y la confidencialidad. En § 2.2.3.1 siguiente se analizará la problemática de la anonimidad y la pseudonimia en *blockchain*.

Con relación al control de *privacidad* del contrato, Arcari propone entender gráficamente la *privacidad* en *Smart Contracts* como si fuera una muralla alrededor del contrato, con un único acceso, y donde las partes tienen la posibilidad de abrir la reja y permitir que terceros, en ciertas condiciones, ingresen al contrato –i.e., Oráculos, árbitros ^[397] al otorgárseles una llave privada. En este sentido, en materia de contratación inteligente efectivamente las partes *controlan* el contrato, y pueden decidir dar o permitir acceso al mismo a terceros, y de hecho en la mayoría de los *Smart Contracts*, han sido programados de modo tal de permitir dicho acceso a una serie de partes autorizadas. Imagine, lector, que el *Smart Contract* es un Google Docs: se pueden otorgar distintos permisos a otros usuarios.

Ahora bien, hay otra particularidad: el código del contrato es públicamente visible por todos –si corre en una *blockchain* pública como Ethereum, por supuesto– y, por ende, el contrato *per se* no es ni será nunca confidencial ^[398]; las partes no son las únicas que lo conocen toda vez que una *blockchain* pública es, justamente, pública, y todos pueden ver a las partes involucradas (i.e., sus llaves públicas) y las cantidades de tokens, *altcoins* ^[399], bitcons o Ethers transferidas entre ellas desde que el contrato se inició. Lo anterior no impide que los *Smart Contracts* pueden ser *ab initio* programados de modo tal de requerir autorización para que terceros extraños no puedan acceder a ninguna otra información que contengan ^[400].

2.2.3.1. Anonimidad y pseudonimidad en la *blockchain*: encriptado asimétrico y On-Chain Analytics

Existe una creencia general equivocada, que sostiene que Bitcoin, Ethereum, NEM y tantas otras *blockchains* son anónimas e intraceables. Nada más alejado de la realidad. Todas las *blockchains* permiten justamente dejar un registro –ver una trazabilidad total de las transacciones, con sus fechas y montos–, y asociar tales transacciones a las llaves públicas entre las cuales tuvieron lugar –éstas no son necesariamente conocidas por todo el mundo ^[401]. Por tanto, es técnicamente más correcto hablar de *pseudonimidad* ^[402].

Los desarrollos de encriptado asimétrico no son nuevos, y son una característica esencial de todas las *blockchains* públicas. Es la tecnología que permite que la identidad real de un usuario de *blockchain* sea protegida, del mismo modo que se protegen los números de una tarjeta de crédito cuando se hace una compra online a través de una línea no segura ^[403]. En la criptografía de llave pública, un vendedor on line tiene dos números, muy largos, uno es una llave pública –todo el mundo puede verla–, y el otro es una llave privada –secreta–; parecen ser números aleatorios, pero no lo son: son elegidos cuidadosamente de modo tal que cualquier mensaje pueda ser encriptado y desencriptado con dos operaciones muy simples ^[404].

En el caso de Bitcoin, por ejemplo, se dice que las identidades de sus dueños están *protegidas* ^[405], porque las direcciones que registran la tenencia de los bitcoins están criptográficamente protegidas –mediante un algoritmo llamado *ECDSA* ^[406] – con una llave pública, y sin su correspondiente y única llave privada ^[407], es absolutamente imposible mover, transferir o disponer de los bitcoins “aparcados” en la llave pública del usuario. Así, el tenedor de una llave privada no necesita entregar información personal –i.e. su identidad– para demostrar que realmente posee las bitcoins “registradas” o “asociadas” a una determinada llave pública ^[408].

Ahora bien, existen múltiples formas de asociar una llave pública a una identidad real, de hecho hay empresas que ofrecen estos servicios ^[409]. Y

también se ofrecen servicios en la dirección contraria, buscando dificultar que se asocien identidades a llaves públicas [\[410\]](#). También es posible crear una llave pública *para cada* transacción, de modo tal de dificultar que se extraigan patrones entre llaves públicas que puedan permitir conocer la identidad real del usuario [\[411\]](#).

En efecto, existe ya un nuevo sector de negocios, que puede denominarse *On-Chain Analytics*, que extrae conocimiento de los distintos datos públicos registrados en una *blockchain*, previo procesamiento [\[412\]](#). Las empresas que operan en este nuevo sector, toman información vinculada a los detalles de cada bloque (sello de tiempo, pago de comisiones y *black rewards* a mineros, direcciones, usuarios), de cada transacción (direcciones entre las que se hicieron, cantidades, cuánto tiempo retuvieron las criptomonedas –*UTXO data* [\[413\]](#) –, etc.), y los *Smart Contracts* utilizados, y de allí extraen patrones de quién, cómo y cuándo utiliza criptomonedas.

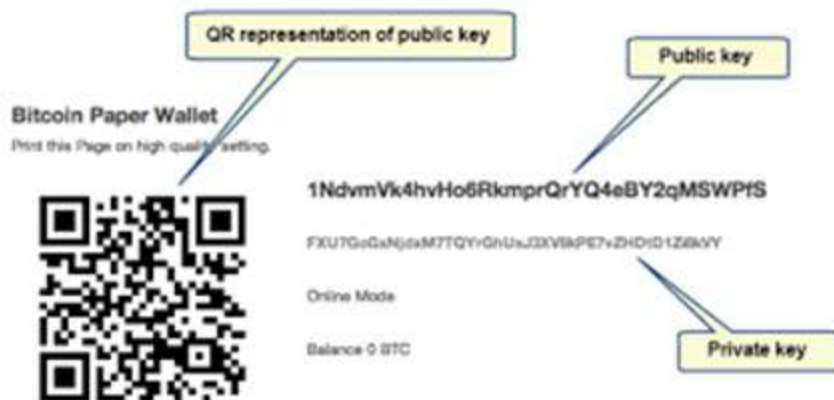
Cada día, distintas propuestas de soluciones tecnológicas se van desarrollando –siempre siguiendo a Arcari– que permiten seguir avanzando en la disciplina y en las novedosas cuestiones vinculadas a la privacidad en *blockchain*, tecnología ésta que recién transita por su infancia.

En efecto, por un lado, la confidencialidad puede “fortalecerse” con técnicas de encriptación *on-chain*, tales como Key Definition Functions (KDF) o protocolos de Confidential Transaction (CT) [\[414\]](#). También se han propuesto nuevas formas de “camuflar” a los *Smart Contracts* y de ofrecer *transactional privacy* [\[415\]](#).

2.2.3.1.1. Llave pública y billeteras digitales – Wallets

Útil es recordar cómo se ve una llave pública o *dirección* en una *blockchain*:

Imagen 1: llave pública



Muy vinculado a las llaves públicas (y privadas), está el concepto de las billeteras digitales o *wallets* [\[416\]](#).

Las *wallets* son un programa de software que almacena llaves públicas y llaves privadas, y que interactúan con varias *blockchains* –Bitcoin, Ethereum, NEM, etc.–, permitiendo a los dueños de las *wallets* enviar y recibir criptomonedas y ver el balance diario de criptomonedas en su/s llave/s pública/s –i.e. en sus direcciones, si se prefiere

Es importante entender que una *e-wallet* no funciona como una billetera en el sentido tradicional y *off-chain*. En efecto, la *wallet per se* no contiene criptomonedas; sólo contiene la/s llave/s pública/s y privada/s de una persona. Cuando una persona envía a otra bitcoins o cualquier otra criptomoneda, lo que en realidad hace es (i) firmar una transferencia “dominial” de dichas monedas a favor de la dirección –llave pública– de una *wallet* de otra persona, y (ii) quien las recibe, para poder gastarlas –i.e., transferirlas nuevamente– debe a su turno ingresar –i.e. firmar– con su llave privada, que está criptográficamente asociada a su llave pública contenida en la *wallet*, la que también le permite ver el saldo de todas sus tenencias.

Generalmente las billeteras pueden ser un software, un hardware, o simplemente un papel a donde están anotadas la llave pública y privada de una persona.

Cuando la billetera es un software, pueden funcionar como un software

para computadoras de escritorio, y sólo pueden accederse desde la computadora en la cual se descargaron. También pueden funcionar como una aplicación móvil, que se descarga y se utiliza desde el teléfono. O pueden ser wallets online, alojadas en la nube, y accesibles desde cualquier dispositivo [\[417\]](#).

Cuando la billetera es un hardware, la llave privada es almacenada normalmente en un pen drive, con lo cual la llave privada está en un “*depósito off line*”.

Cualquiera sea el tipo de *wallet* empleado, si uno pierde la llave privada [\[418\]](#) –o se hace pública–, no hay forma de recuperar las criptomonedas [\[419\]](#) o de frenar su uso indebido. Recordar que el dominio de un criptoactivo se acredita y se ejercita sólo con la llave privada criptográficamente asociada a una llave pública que, según la *blockchain* de que se trate, tiene asociado el criptoactivo, por tanto, la llave privada no es una contraseña común y cualquiera y su pérdida (o robo) puede causar un daño irreparable [\[420\]](#).

Ahora bien, una persona humana (o jurídica) puede tener cuantas direcciones –i.e., llaves privadas– quiera, y en esas direcciones tener criptomonedas que son en sí totalmente trazables [\[421\]](#), pero como se adelantó, no es fácil asociar la llave pública a una identidad real [\[422\]](#). Ahora bien, una vez que se asocia una llave pública a una identidad real, tampoco hay forma alguna de borrar el historial de transacciones, con lo cual se puede saber el origen (lícito o ilícito) de esas transferencias [\[423\]](#). Y esto es, también, *revolucionario*. Por tomar Bitcoin, permite auditar el camino inverso de transacciones de un modo que es, precisamente, inmutable, aunque no necesariamente implica llegar, en todos los casos, al destinatario final [\[424\]](#).

Una de las formas de *trackear* la actividad en Bitcoin es mediante el *clustering*, que consiste en mirar de cerca la actividad en una *blockchain* aplicando *Machine Learning*, y de tal modo intentar detectar *cuentas* que

parecen ser de una misma *wallet*, por ende, controladas por una sola persona o entidad ^[425]. La prestigiosa MIT TECHNOLOGY REVIEW lo pone en estos términos:

“Multiple addresses initiating the same transaction might begin to look like one person or organization consolidating smaller funds into one bigger pot, for example. Another telltale sign is when change from a Bitcoin transaction is routed back into an account different from the one where the funds started off. In time, the chaos resolves itself into regular patterns. **Once multiple accounts have been linked to the same owner, you can try to figure out who that owner is.** Linking Bitcoin accounts to real-world identities is possible because information tends to leak out. Regulated cryptocurrency exchanges—generally those in the US or Europe—must follow **know-your-customer** and **anti-money-laundering** rules, which require people to hand over identification before using their services.” ^[426] (el resaltado me pertenece)

Como síntesis de los varios asuntos vinculados a la privacidad en los *Smart Contracts*, a medida que nuevas tecnologías –tales como las ya analizadas ZKPs– y nuevos servicios –como Zcash ^[427] o Monero ^[428] – se empleen para potenciar o proteger la privacidad, el *clustering* será menos eficiente. Pero también serán cada vez más supervisados –y eventualmente sancionados– los actores vinculados al ecosistema *blockchain* que no cumplan con las normas de KYC y AML, como ilustra el caso del Exchange ruso BTC-^[429]
e

2.2.4. *Ejecutabilidad (o cumplimiento forzoso o automatizado).*

La última característica que Szabo señalaba como propia y fundacional de

los *Smart Contracts* es su *enforceability*, que podría traducirse como su cumplimiento forzoso [\[430\]](#), o automático, o mejor dicho, automatizable [\[431\]](#), como la lógica consecuencia que deriva de iniciar un contrato inteligente en una *blockchain*: lo programado –sea lo que sea– se auto-ejecutará, sin ninguna intervención de la contraparte, y sin poder revertirse la operación debido a la inmutabilidad de la *blockchain*, salvo que el programa haya sido escrito previendo formas de reversión.

Lo expuesto, a su turno, se vincula con un problema también propio, pero más amplio, vinculado a los contratos inteligentes: la consecuente posibilidad (real o no) de demandar jurisdiccionalmente la nulidad [\[432\]](#) de una obligación codificada en una cadena de bloques, ejecutada mediante un contrato inteligente que no es reversible.

En un sentido más amplio, se ha sostenido que un contrato inteligente puede funcionar mal por razones inherentes al código del contrato o a la plataforma en la que está siendo ejecutado, o, inversamente, puede haber funcionado adecuadamente bien, pero ciertas razones o causas extrañas al contrato y a la plataforma hacen que exista un incumplimiento contractual [\[433\]](#). En este sentido, el incumplimiento o el cumplimiento defectuoso de una obligación contractual automatizada puede habilitar para la parte perjudicada medios tradicionales –i.e. jurisdicción común, o de excepción, arbitraje– o medios no tradicionales, que pueden ser incluso nativos en una plataforma dada [\[434\]](#), como son los casos de *Aragon* y *OpenBazaar* que más abajo se analizan [\[435\]](#).

Ahora bien, en términos más analíticos y también más polémicos, la ejecutabilidad de un contrato inteligente dispara otros muchos interrogantes jurídicos: ¿los *Smart Contracts* son contratos para la Ley? ¿Se necesita el dictado específico de una ley que los califique legalmente como un contrato [\[436\]](#)? ¿Es (o será) posible demandar judicialmente su nulidad, o su incumplimiento esencial [\[437\]](#), o daños y perjuicios con título, causa u origen en un cumplimiento que se aparta de lo pactado?

A su vez, cuando haya consumidores involucrados, ¿un *Smart Contract* puede ser considerado un contrato celebrado fuera del establecimiento comercial ^[438], o celebrado a distancia y sujeto a la facultad de revocación del consumidor ^[439]? ¿Iniciar un contrato inteligente en una *blockchain* equivaldrá a una celebración por escrito de un contrato ^[440]? En tal caso, ¿deberían los proveedores de servicios digitales informar a los consumidores que los *Smart Contracts* son –generalmente– irreversibles ^[441]? ¿Quién asume el riesgo de un error en la codificación, como ocurrió con *TheDAO*?

Todos estos interrogantes serán respondidos más adelante en el Capítulo siguiente, pero reténgase aquí que el rasgo esencial de los *Smart Contracts* – quizás su mayor atractivo – es la imposibilidad *técnica* de incumplirlos, toda vez que el código de un *Smart Contract* se ejecuta de manera autónoma una vez iniciado, y salvo que se haya previsto desde su diseño la posibilidad de detenerlo, se auto-ejecutará por si mismo en la *blockchain* ^[442].

2.3. Usos actuales de Smart Contracts. Smart Contracts híbridos

El CARDOZO BLOCKCHAIN PROJECT señala ^[443] que existen dos grandes campos de uso de los contratos inteligentes.

Por una lado, se los utiliza para transacciones simples, donde las partes confían y delegan enteramente el cumplimiento en *Smart Contracts*, sin ni siquiera celebrar un contrato convencional. Así, el código del programa regula la relación comercial en todas sus partes, incluyendo pagos, transferencia de activos, y términos y condiciones asociados. Ejemplos actuales de este uso novedoso de los de *Smart Contracts* son *Ujo Music* ^[444], *OpenBazaar* ^[445] y *SafeMarket* ^[446].

Por otro lado, los *Smart Contracts* también se pueden utilizar para codificar una parte de las obligaciones contractuales de una parte –las que se puedan

automatizar ^[447] –, mientras que otras obligaciones se mantienen en la esfera convencional tradicional ^[448] –i.e., declaraciones y garantías, ley aplicable, y procedimientos para resolver controversias– ^[449] . Se trata de *Smart Contracts híbridos*, en los que el contrato convencional expresamente hace referencia al *Smart Contract* y contextualiza cómo esa porción de obligaciones se incrusta dentro de un acuerdo comercial más amplio ^[450] .

En estos *Smart Contracts híbridos*, las partes voluntariamente elijen delegar el cumplimiento de una parte de sus obligaciones en un programa de computación que se auto-ejecuta de manera descentralizada en una *blockchain*.

Si hubiera un conflicto, las partes podrán siempre renegociar/ajustar el contrato convencional subyacente, o, si es posible, buscar la forma tecnológica de revertir los efectos del *Smart Contract* autónomo. Sin embargo, la dificultad asociada a ésta última situación puede ser justamente lo que las inclinó *ab initio* a utilizar un contrato inteligente e irreversible, que (i) libera a las partes de la carga de supervisar el cumplimiento de la contraprestación; y (ii) se ejecutará siempre, si se cumplen las condiciones programadas. Incluso, las partes pueden haber programado al contrato inteligente de modo tal que, recurriendo a Oráculos, modifique o se adapte ^[451] a una serie de opciones de cumplimiento programado, de acuerdo a la variación de condiciones exógenas al contrato inteligente, pudiéndose incluso recurrir a datos tomados o informados por sensores con IoT, o IIoT, etc ^[452] .

Naturalmente, la tecnología permite testear el código de un *Smart Contract* –así como cualquier tipo de software puede ser testeado ^[453] – antes de ejecutarlo en una *blockchain*, de modo de verificar que se ejecuta tal como fue acordado por las partes.

Evidentemente, cada vez que una empresa explore la posibilidad de celebrar *Smart Contracts* híbridos, sus abogados deberán necesariamente involucrarse en el asunto, y trabajar cabeza a cabeza con el equipo de programación, para asegurar que el código refleje lo pactado en el contrato

convencional subyacente [\[454\]](#).

2.4. *Desmitificando a los Smart Contracts*

Ahora bien, analizadas las definiciones de los *Smart Contracts*, y planteadas sus principales características y vistos algunos usos actuales, luce conveniente ahora situarlos en la complejidad del mundo real, y desmitificarlos [\[455\]](#).

2.4.1. *Creación de tokens vs. transferencia de tokens vía Smart Contracts*

Como regla general, los *Smart Contracts* sirven sólo para transferir tokens, o criptomonedas. Los *Smart Contracts* no crean nuevos tokens [\[456\]](#). Cuando se dice que un *Smart Contract* se auto-ejecutará, lo que se quiere decir en realidad es que *transferirá* los tokens que controle, si ocurren determinadas condiciones pre-establecidas, y a favor de determinada llave pública pre-establecida [\[457\]](#).

2.4.2. *Codificación deficiente o inexacta de un Smart Contract*

Como todo software, un *Smart Contract* está sujeto al riesgo de codificación *deficiente* o *inexacta*. Codificación deficiente hace referencia a la existencia de errores de programación en el código de un *Smart Contract*, llamados informalmente *bugs*.

Si un contrato inteligente tiene un error de codificación, se ejecutará mal, de modo tal que la auto-ejecución no garantiza el cumplimiento perfecto de la prestación codificada [\[458\]](#). Es prácticamente imposible garantizar que un código de programación no tendrá *bugs*, con lo cual es importante *auditar* el código y probar su funcionamiento *antes* de desplegarlo en la vida real. Las

partes contratantes debieran dejar previsto “cláusulas de escape” para corregir los eventuales *bugs* que aparezcan, de lo contrario, la parte perjudicada debiera acudir a la Justicia para solicitar la reparación de los perjuicios causados [\[459\]](#). Se volverá sobre esto en el Capítulo siguiente.

Por otro lado, la codificación puede no contener errores, sino ser inexacta, en el sentido de no reflejar adecuadamente la intención de las partes que lo utilizan.

El programador –o la empresa de programación– contratado para escribir el código de un *Smart Contract* puede no entender cabalmente la intención de las partes, actuando con negligencia o quizás dolosamente. A menos que las partes sean programadores y puedan ellos mismos verificar qué dice el código, deberán recurrir al servicio de terceros para corroborar que el código refleja lo que las partes quisieron que reflejara [\[460\]](#). Además, es prácticamente imposible codificar de manera anticipada todos los futuros escenarios posibles, lo que impone aceptar que un contrato inteligente pensado adrede para durar en el tiempo no podrá probablemente adaptarse a (todas) las nuevas circunstancias imprevistas.

Pues bien, debe aceptarse entonces que los errores de codificación son harto frecuentes y prácticamente inevitables [\[461\]](#). Sin embargo, existen mecanismos para detectarlos: herramientas de análisis estático que pueden detectar patrones conocidos de errores, y herramientas de verificación formal, que permiten garantizar que un contrato inteligente se comportará de modo correcto [\[462\]](#). Por otro lado, existen herramientas para realizar ingeniería inversa en los *Smart Contracts*, que permiten auditar el código fuente de un contrato inteligente [\[463\]](#).

2.4.3. Traducción del lenguaje natural: sus limitaciones

Normalmente, las partes que decidan implementar un contrato inteligente para automatizar determinados aspectos de su relación, delinearán el alcance y características que el contrato inteligente deberá tener y cumplir en un

documento escrito precedente, en lenguaje natural, que luego debe ser “traducido” al lenguaje que procesan las computadoras ^[464]. Eliza Mik señala, con razón, que este proceso de “traducción” desde el lenguaje natural al lenguaje de programación –*source code*– que utilice el contrato inteligente es harto complejo y suele ser subestimado. Es un proceso manual, donde la supervisión del empleo y el significado de los términos legales por parte de abogados es absolutamente crucial.

Por otro lado, la terminología legal sigue siendo un tipo de lenguaje natural calificado, que no es tan fácilmente codificable, y que requiere de una interpretación previo a su codificación ^[465]. Normalmente, lo que ocurre es que los Tribunales interpretan ^[466] los contratos *ex post*, cuando surge el conflicto y se judicializa. Por tanto, los programadores que codifican *Smart Contracts* requieren el acompañamiento de Abogados, quienes deben *ex ante* explicar los efectos de los conceptos jurídicos involucrados, prestando atención al contexto en el cual los conceptos jurídicos se utilizan ^[467] y teniendo en cuenta la ambigüedad de las palabras.

No obstante lo anterior, Koulu ^[468] sostiene que los contratos inteligentes operan con una lógica similar a la de los contratos convencionales, en el sentido que es siempre necesaria la intención común de las partes para vincularse, y en los *Smart Contracts* esto suele ocurrir cuando las partes “transfieren” tokens o criptomonedas al *Smart Contract*. Incluso acuña un término que puede ser interesante explorar: *Legal Programming*.

2.4.4. Codificación directa de obligaciones contractuales

Es posible también que las partes no celebren un documento precedente delineando el alcance del futuro contrato inteligente, sino que elijan directamente codificar sus obligaciones ^[469], para eliminar los riesgos asociados a la codificación del lenguaje natural y/o la ambigüedad de las palabras.

Esto implica asumir que los Abogados aprendan a programar, o que los

programadores aprendan Derecho, lo que seguramente ocurrirá en el futuro, pero no es una realidad cotidiana en el presente. Lo que sí puede hacerse en el momento presente es redactar contratos teniendo en cuenta que serán (o que podrían ser), en alguna de sus partes, susceptibles de codificarse con *Smart Contracts* [\[470\]](#). Surden, según se analizó más arriba, denominaba esta práctica *data-oriented contracts*.

Mik afirma, con razón, que la ambigüedad de las palabras en sentido legal no es necesariamente un defecto inadmisibles, tal como los programadores lo consideran [\[471\]](#). En efecto, si bien la ambigüedad puede generar conflictos eventuales respecto al alcance de las obligaciones de las partes, también permite cierto grado de flexibilidad, y adaptarse a nuevas circunstancias imprevistas, y de hecho, muchas cláusulas contractuales son redactadas con términos amplios, a propósito. En la terminología contractual muchas veces se debe balancear la certeza de las palabras contra la adaptabilidad del contrato, especialmente cuando los contratos son de largo plazo, y con mucha razón protesta Mik cuando afirma que los contratos inteligentes pueden requerir formalizar lo informal, o cuantificar lo cualitativo [\[472\]](#). Menuda tarea.

Por otro lado, es prácticamente imposible prever en un contrato convencional absolutamente todos los escenarios futuros posibles, y lo mismo se predica de un contrato inteligente. Para prever todas las opciones posibles, éstas deben codificarse, lo que implica largas líneas de código y la creciente posibilidad de cometer un error en la codificación.

Para finalizar, Mik también señala que no toda obligación es codificable. Cierta tipo de obligaciones, en su esencia, no son susceptibles de codificarse ni de automatizarse ya que requieren el ejercicio del juicio humano [\[473\]](#), mientras que otras, más manuales, sí lo serán.

2.4.5. *Criminal Smart Contracts*

Desmitificar a los contratos inteligentes implica también señalar que existen quienes creen que los *Smart Contracts* pueden ser o serán utilizados

para el mal, configurando verdaderos *Criminal Smart Contracts* ^[474].

Blockchain en sí, especialmente Bitcoin, también ha sido utilizada para monetizar actividad legal, a través de *ransomware* ^[475], o para pagar la adquisición de bienes ilegales ^[476], y para el lavado de dinero ^[477]. Ahora bien, a medida que la utilización de *Smart Contracts* se masifique, se ha señalado que también podrían ser técnicamente programados para cometer actos ilícitos, como por ejemplo, robar llaves privadas, filtrar documentos confidenciales, y retribuir delitos por encargo ^[478].

En este sentido, puede tomarse el caso de Darkleaks ^[479] que sirve como un mercado descentralizado para la filtración pública y anónima de secretos que van desde películas, secretos comerciales, código fuente de software, diseños industriales, etc. ^[480].

Siguiendo a Juels, es posible hoy programar contratos inteligentes *malos* para solicitar el robo de una llave privada que corresponde a una llave pública, o lo que es lo mismo, la llave de la bóveda que aloja criptoactivos, utilizando técnicas como el zk-SNARKs ^[481]. Esto implica, lógicamente, que los contratos inteligentes *buenos* hoy ya deben ser programados previendo esta posibilidad cierta de ataque.

Como primera medida de seguridad, se ha intentando recurrir a “listas negras” ^[482] de monedas –que se sabe que fueron robadas–. En esta misma línea, en Agosto de 2019 el Departamento del Tesoro de EE. UU ha publicado llaves públicas de Bitcoin que pertenecían a presuntos narcotraficantes ^[483]. Como segunda medida, Juels propone crear un sistema en el cual un conjunto de entidades a ser designadas sean facultadas para remover criminal *Smart Contracts* de la *blockchain*, sin requerir que sus usuarios se identifiquen, aunque también reconoce que la posibilidad técnica de poder implementar un sistema así es una cuestión aún abierta ^[484].

2.4.6. Problemas para la ejecución judicial de Smart

Contracts

Finalmente, para el caso que el *Smart Contract* no funcione, no opere, o no se ejecute totalmente [\[485\]](#) tal y como se pensó que lo haría, las partes “*programantes*” quizás deban recurrir al servicio de administración de justicia convencional, asumiendo que conocen las identidades de (todas) las partes contratantes. Se ha sostenido que una forma de darle “ejecutoriedad legal” a un *Smart Contract* es incluir en él una referencia al contrato *off-chain*, y viceversa, práctica denominada *integración dual* [\[486\]](#). En éste sentido, véanse las propuestas de valor de Common Accord [\[487\]](#) y Legal Markdown [\[488\]](#).

Sin embargo, es evidente que la tutela jurisdiccional tendrá un limitado alcance en la materia [\[489\]](#). Alguna doctrina sostiene que deberán aplicarse a los incumplimientos de *Smart Contracts* (sic) –asumiendo que ello sea posible dada su ejecución automática [\[490\]](#)– los mismos principios y reglas que se aplican a los incumplimientos contractuales convencionales [\[491\]](#). En este particular, sería computacionalmente imposible afectar o modificar retroactivamente una transacción ya ejecutada vía *Smart Contract*, ya que el programa está desplegado en una *blockchain*, con lo cual el único remedio posible –si se conoce la identidad de las partes– sería ordenar judicialmente la programación de un nuevo contrato inteligente reverso [\[492\]](#).

Otros sostienen que dado el carácter territorial de la jurisdicción, sería imposible poder demandar a la contraparte en un *Smart Contract* descentralizado, salvo que algún “operador” [\[493\]](#) de la red permita identificarlo [\[494\]](#), o que se pueda identificar al “creador” de una *blockchain* [\[495\]](#).

Además, no serían menores las dificultades de un Tribunal a la hora de interpretar un contrato inteligente, escrito en un lenguaje de programación normalmente desconocido para un Juez, y más allá de las pericias técnicas que se puedan disponer a pedido de parte o como medidas para mejor

proveer para intentar descifrar qué dice el código de un contrato inteligente ^[496]. Innegablemente, el código de programación del *Smart Contract*, cualquiera sea el lenguaje utilizado, deberá ser traducido a lenguaje natural para que los Jueces puedan entenderlos ^[497].

2.5. *Juez competente, ley aplicable y resolución de controversias en un entorno de blockchain-based Smart Contracting*

Además de las (grandes) limitaciones técnicas para codificar obligaciones, de los casi inevitables errores de codificación asociados al *arte de programar*, de la necesidad de tener que recurrir a los Oráculos para obtener información *off-chain*, y de, incluso, la posibilidad de programar los llamados *Criminal Smart Contracts*, los *Smart Contracts* plantean otros interesantes problemas (y también novedosas soluciones), vinculados a la gestión y resolución de conflictos en entornos *blockchain*, que se inscriben en una categoría analítica más amplia, la de gestión de conflictos online, comúnmente denominada *Online Dispute Resolution* ^[498].

Se ha afirmado que la infraestructura legal actual no podrá, eficientemente, resolver dichos conflictos (i) al no poder identificar a las partes que celebran transacciones sobre criptoactivos ^[499] y, además, por (ii) el posible carácter transnacional de la disputa agravado por el hecho de que muchas veces el monto del conflicto no justificaría el acceso a la justicia.

En este sentido, se ha puntualizado que las cláusulas de resolución de conflictos en contratos *on line* deben ser repensadas si el contrato puede auto-ejecutarse sólo si se dan ciertas condiciones, e incluso, tales cláusulas pueden perder utilidad en contratos comerciales multi-jurisdiccionales, en la medida que la resolución del eventual conflicto pueda ser automatizada ^[500]. Como solución, se ha propuesto un enfoque de *Justicia Distribuida* que seguidamente se analizará en profundidad.

2.5.1. *Justificantes de una Jurisdicción Distribuida*

En la visión de Kaal y Calcaterra^[501], la lógica subyacente a la necesidad de una *Jurisdicción Distribuida* es la siguiente: (i) la ausencia de un mecanismo de resolución de controversias eficiente en *blockchains* – públicas–, a largo plazo terminará afectando la confianza descentralizada que la *blockchain* permite; y (ii) la ausencia de medios jurisdiccionales para resolver conflictos generados por *Smart Contracts*, puede también provocar la pérdida de confianza de los consumidores y la consecuente no utilización de los contratos inteligentes. Ambos déficits, a su turno, pueden afectar el desarrollo de la criptoeconomía.

A la lógica antes expuesta, se deben sumar dos factores muy importantes. En primer término, la separación entre identidades físicas y digitales producto de la anonimidad relativa en la criptoeconomía afectará también a los mecanismos tradicionales y jurisdiccionales de resolución de conflictos, que han sido pensados: (i) con lógicas de competencia territorial^[502] –que no tienen un correlato en la economía digital^[503] donde surgirán contratos inteligentes con marcado carácter *supra-nacional*^[504] –, (ii) para identidades *off-chain*, que tampoco están presentes en la criptoeconomía debido a la pseudonimia^[505], y (iii) para contratos convencionales, que son muy diferentes a los contratos inteligentes encriptados y descentralizados.

En segundo término, existe muy poca jurisprudencia que aborde específicamente la *blockchain* y los *Smart Contracts*, lo que genera incertidumbre –i.e., inseguridad jurídica–, aun cuando esta tecnología no es muy distinta de cualquier otro software virtual. Por otro lado, los registros distribuidos no existen en el mundo físico, y por ende no tienen una ubicación determinada, a lo que se suma que los nodos de una *blockchain* pueden estar localizados en cualquier parte del mundo, con lo cual las transacciones estarían sujetas a la ley aplicable a cualquier nodo de la red^[506].

Por tales motivos, es que los autores citados proponen un interesante enfoque de gobernanza *intra-blockchain*, capaz de brindar soluciones especiales para un nuevo entorno transaccional de *blockchain-based Smart*

Contracting que, sin dudas, es *muy* especial [\[507\]](#). Ponen Kaal y Calcaterra el énfasis en que casos como el *TheDAO* serán cada vez más usuales, y en que los *Smart Contracts* traerán inevitablemente nuevos tipos de conflictos, potenciados por el encriptado asimétrico, el *hashing* y la anonimidad relativa.

2.5.2. Características de una Jurisdicción Distribuida

Una *Jurisdicción Distribuida* como proponen Kaal y Calcaterra asume dos realidades: (i) que la existencia de errores en la codificación de *Smart Contracts* es innegable, como así también es innegable que es imposible que todas las posibles formas de incumplir un contrato inteligente puedan ser codificadas *ex ante facto*, debido a la propia limitación humana, y (ii) el caso *TheDAO* sobra como muestra de que lo anterior es, efectivamente, innegable.

Desde ese punto de partida sociológico, se afirma que la forma de resolver las eventuales disputas generadas por *Smart Contracts* debe, necesariamente, ser *intra-blockchain*, es decir, la forma de resolver los conflictos (i) no puede ser exógena, sino que debe ser endógena y dentro del mismo entorno *blockchain*, para poder mantener la anonimidad propia del entorno, y (ii) requiere un sistema de administración –o de gobierno, si se quiere– programado dentro de la o las *blockchains* de que se trate, como por ejemplo ofrece la red *Aragon* que se verá más abajo [\[508\]](#).

En la visión de Kaal y Calcaterra, una *Jurisdicción Distribuida* debiera ser: (i) una plataforma *open source* que garantice la anonimidad; (ii) a la que las partes de un *Smart Contract* que tengan un conflicto real puedan voluntariamente someterse; (iii) exista una reputación de cada árbitro –cuya identidad es desconocida– de modo que las partes puedan elegir al que consideran más adecuado; (iv) los árbitros presentarían sus laudos a la comunidad de árbitros, la que podría confirmarlos o rechazarlos, afectándose lógicamente la reputación del árbitro en función del dictamen final de la comunidad sobre cada laudo; y (v) los laudos no serían nunca finales y definitivos, pudiéndose reabrir el caso [\[509\]](#).

2.5.3. Casos de uso. Say (again) hello to Ricardian

contracts!

Señalan Kaal y Calcaterra los ejemplos de *Aragon* y de *OpenBazaar*.

El primero utiliza una forma de jurisdicción digital distribuida, administrada por una sistema de jueces y reguladores anónimos, cuyo poder depende de su tenencia de tokens de la red, y de la reputación que construyan resolviendo conflictos. *Aragon* sacó a la venta su token, *ANT* en Mayo de 2017, y levantó 25 millones de Dólares en 15 minutos [\[510\]](#), el cuarto evento de crowdfunding más importante de la historia, y el segundo mayor sino se tiene en cuenta *TheDAO*.

OpenBazaar, por su lado, si bien no utiliza *blockchain* y *Smart Contracts* técnicamente hablando [\[511\]](#), sí utiliza una red distribuida y todas las partes y transacciones son anónimas y propone un modelo de contratos *Ricardianos* para resolver disputas, modelo que, para algunos, es la segunda generación de contratos inteligentes [\[512\]](#), y que tampoco son tan nuevos.

En efecto, los contratos *ricardianos* fueron propuestos en 1996 por dos programadores, Ian Grigg y Gary Howland, como parte de un sistema de pagos más amplio llamado *Ricardo* [\[513\]](#) y cuyas características esenciales son:

- i) ser un contrato ofrecido por un emisor a un tenedor;
- ii) por algún derecho de valor tenido por los tenedores, y administrado por el emisor;
- iii) fácilmente legible por humanos como un contrato firmado en papel;
- iv) también legible por programas de computación;
- v) firmado digitalmente;
- vi) que lleva consigo las llaves y la información del servidor; y
- vii) con un identificador seguro y único.

En *OpenBazaar*, se puede recurrir a un tercero, llamado coloquialmente *notario*. Las partes del contrato no están obligadas a involucrar a un notario –

se ahorran ciertas comisiones–, pero si eligen esta opción, entonces un notario verifica que el contrato se firmó y que el vendedor depositó bitcoins como depósito en garantía –*escrow account*–. Si el comprador está satisfecho, entonces se libera la garantía del vendedor; si hay conflicto, el notario actúa como árbitro. Durante todo el proceso, se mantiene la anonimidad de las partes –más técnicamente, la pseudonimidad mediante la utilización de llaves públicas–, y los *notarios* son aleatoriamente designados, aunque existen pools de notarios con *expertise* particular a disposición de las partes contratantes [\[514\]](#).

OpenLaw [\[515\]](#) es otra plataforma de *Smart Contracts* que desarrolla el concepto de Contratos Ricardianos, en la que participa como co-founder el prestigioso abogado especialista en *Blockchain*, Aaron Wright, del CARDOZO BLOCKCHAIN PROJECT. La (ambiciosa y muy prometedora) propuesta de valor de OpenLaw es la siguiente:

“OpenLaw is the first fully expressive Ricardian contracting system — the bridge between traditional legal regimes and the Ethereum world. OpenLaw can be used to create binding legal agreements and tie them to the execution of one or more Smart Contracts, including Smart Contracts that create and manage tokens. Through this approach, any token operating on Ethereum and any Smart Contract can be imbued with legal effect.”

2.6. Dapps, DOs, DAOs y DACs

Sin dudas, si la nueva disciplina del *Smart Contracting* es de por sí interesante para el Abogado, las (inmensas) posibilidades que se abren cuando los *Smart Contracts* comienzan a interactuar autónomamente entre ellos, formando DAOs y DACs [\[516\]](#), son simplemente alucinantes, bordeando la ficción, especialmente para el autor, que hace 10 años da clases de Sociedades. Pero el futuro llegó hace rato, y las Dapps, DOs, DAOs y DACs ya están aquí.

Hace 6 años, en 2014, Vitalik Buterin daba las primeras definiciones de las Dapps en un controvertido artículo, titulado *DAOs, DACs, DAS and more: an incomplete terminology guide* [\[517\]](#).

Allí se precisaba que una Dapp –*Decentralized Application*– es una variación de un *Smart Contract*, es decir un mecanismo que involucra activos digitales y dos o más partes, donde alguna o todas las partes afectan activos digitales, los que son automáticamente distribuidos entre las partes de acuerdo a una fórmula basada en ciertos datos que, al momento de iniciar el contrato, no son conocidos.

La Dapp es similar a un *Smart Contract*, pero con dos diferencias: (i) puede haber un número ilimitado de participantes de cada lado del contrato y (ii) no tiene necesariamente que estar vinculada a transacciones financieras.

Las Dapps son a su vez clasificables en dos tipos de clases: (a) totalmente anónimas, o (b) basadas en reputación, a donde algunos nodos siguen la performance de otros, con el fin de mantener la confianza en ellos.

Luego, Buterin también definía a las DOs –*Decentralized Organizations*– como una organización en la que los humanos participan de acuerdo a las reglas fijadas en el protocolo programado –como si fuera el Estatuto Social de una sociedad anónima, o el Estatuto Social de una asociación civil–, pero con la particularidad que dicho protocolo será aplicado a raja tabla por la *blockchain*. Toda la estructura convencional de las sociedades y su tipología legal y distintos tipos de organicismos, puede ser *migrada* a una *blockchain*, para que registre las tenencias de los accionistas/asociados, quienes expresan su voluntad –votan– también vía *blockchain*. Lo mismo es predicable respecto de personas jurídicas sin fines de lucro. La DO puede controlar activos digitales, o físicos, en la medida que su código interactúe con tales activos.

Avanzando un poco más, Buterin definió también a las DAOs –*Decentralized Autonomous Organizations*– como el Santo Grial de los *Smart Contracts*. Una DAO es un término genérico, que incluye también las DACs –*Decentralized Autonomous Corporations*–, una especie de DAO.

A diferencia de la DOs, las DAOs y DACs son entidades que viven en Internet, son autónomas, y pueden incluso contratar a personas para que realicen las tareas que ellas no pueden. Las DAOs vendrían a ser los espejos en *blockchain* de una fundación o una asociación civil, i.e. entidades sin fines de lucro, aunque tienen un “capital digital”, y están facultadas por su código

de programación para disponer de dicho capital en ciertas circunstancias, generalmente para retribuir o premiar conductas. En el caso de las DOs, éstas también tienen un capital, pero éste está gestado por humanos que son quienes toman las decisiones al final del día; mientras que el capital “digital” de las DAOs está gestado por el código de la DAOs, de manera autónoma. Ejemplos actuales de DAOs son SolarDAO^[518], DAOStacks^[519], Wings^[520], XWIN^[521], y PieDAO^[522].

El tema comienza a llamar la atención de muchos. Se ha sostenido que 2020 será “*El Año de las DAOs*”^[523]. En opinión personal del autor, la década del 2020-2030 será la *Década de las DAOs*, y recordando el informe de GARTNER antes citado, el mercado de servicios en *blockchain* tendrá un tamaño equivalente a 6 PBIs de Argentina al final de la década. Pero en el corto plazo, i.e., 2020-2023, se comenzará a ver muchísima actividad –i.e., innovaciones incrementales encadenadas, o *incremental on-chain innovations, Io-cl*, como yo las llamo– en materia financiera, en una tendencia que se denomina *Decentralized Finance* (“DeFi”), que combinará *Smart Contracts*, DAOs y, especialmente, una fuerte creencia de *underperformance* por parte de la banca tradicional^[524]. MakerDAO^[525] es un ejemplo exitoso de esta nueva tendencia *DeFi*.

Finalmente, Buterin definió a las DACs como una especie del género de las DAOs, con la diferencia que la DAC paga dividendos, es decir, es (o sería) una persona jurídica digital con fines de lucro, a diferencia de las DAOs que son sin fines de lucro. Buterin señala que el énfasis en los dividendos puede complicar definir situaciones en la que los partícipes reciben *tokens* como dividendo, y estos tokens, a su vez, pueden ser:

- i) meros “permisos de uso” de ciertos activos digitales que integran “el activo digital” de la DAO o de la DAC; o pueden ser
- ii) monedas propias emitidas por la DAO/DAC, o pueden
- iii) ser otras criptomonedas adquiridas, en contraprestación por los bienes y servicios producidos por la DAO/DAC y comercializados a terceros, o

iv) moneda fiat, de curso legal, convencional, emitida por un Estado.

Es útil a los fines pedagógicos traer ahora a colación una segunda definición de una DA y DAOs, y entender el concepto comparándolo con el de sociedad anónima convencional:

“A decentralized organization is a computer program with no single leader, running on a peer-to-peer network that involves a set of users interacting with each other according to protocol programmed through code and enforced on a blockchain.” [\[526\]](#)

*“A decentralized organization **operates under the same basic concepts of a corporation but has a decentralized management structure—eliminating the board of directors, for example.** The structure of a simple corporation has three classes of members: shareholders, a board of directors, and other members involved in the corporate hierarchy. To become a member in the corporation, shareholders purchase a slice of the company. **Investors follow a set of bylaws determining how votes are cast, how they can select the board of directors, and so on.** Other members in the corporation, such as employees, are hired by either directors in the corporation or other employees in the hierarchy. **A decentralized organization involves a set of users interacting with each other and making decisions according to protocol specified in code and enforced on the blockchain.** In a decentralized organization, the contract is coded in the blockchain and maintains a record of each shareholder’s holdings and allows for shareholders to vote on various items through the blockchain. **What distinguishes a decentralized autonomous organization from a decentralized organization is its autonomous capability.** Decentralized autonomous organizations are essentially a set of Smart Contracts that encode the bylaws of the entire organization. This means that the traditional terms that make up a contract are coded and*

*uploaded to the blockchain, creating a decentralized Smart Contract. Unlike the traditional organization, the decentralized autonomous organization does not need to rely on a third party for recordkeeping or enforcement. **The blockchain stores information including how many tokens each participant owns in the company or its bylaws.** When certain pre-programmed conditions are satisfied, the decentralized autonomous organization automatically executes contractual clauses in the blockchain. In this way, decentralized organizations and decentralized autonomous organizations are similar. However, although **decentralized organizations are also made up of Smart Contracts, human intervention in some way is still required.** Decentralized organizations like the DAO depend on human involvement on each end of various transactions. **In contrast, a decentralized autonomous organization is designed to run autonomously on a blockchain and is solely controlled by code, without any need for human involvement.** [527]” (el resaltado es mio).*

2.6.1. Round 1: Enter The DAO

Se ha señalado con gran razón que el Derecho tiene amplia tradición en reconocer que ciertas *ficciones* jurídicas pueden tener la misma capacidad legal que los seres humanos [528]. En efecto, esa es precisamente la lógica que subyace en todo el Derecho Societario, desde el Derecho Romano en adelante, con la particularidad de que en las personas jurídicas que nuestra legislación reconoce, siempre hay en el *back-office* personas humanas [529].

En efecto, se ha señalado que desde antaño, diversas agrupaciones combinan la posibilidad de aglutinar capital y habilidades humanas, las que con ayuda de técnicas asociadas han evolucionado hasta conformar patrimonios auto-gestantes, escindidos de los sujetos que originalmente acuden a su formación [530]. Los antecedentes más antiguos tienen origen babilónico -1.900 AC-, pero también los griegos recurrieron a esta técnica;

los romanos la perfeccionaron y modelaron en un modo que ha llegado, con pequeños ajustes bárbaros, hasta el Siglo XIII [\[531\]](#). Ya en el Siglo XV se gestaron las primeras Compañías que sí son antecedente directo de nuestras sociedades comerciales [\[532\]](#).

¿Acaso en el Siglo XXI habrá llegado el momento de ampliar la *ficción* de la personalidad jurídica para incluir a las DAOs y DACs, *entidades* desprovistas de personas humanas? Bayern no duda en contestar afirmativamente a la cuestión planteada, y de hecho afirma que ello ya ha ocurrido [\[533\]](#), pero también plantea interesantes preguntas que nos llevan a un plano más Iusfilosófico: ¿es conveniente o necesario aplicar el sistema legal convencional a estas nuevas entidades? ¿Qué tiene de malo que exista una entidad autónoma que persiga su propio fin sin rendir cuentas a nadie? ¿Será un problema que tal entidad tenga empleados humanos? Si fueran configuradas como entidades sin fines de lucro, ¿no podrán ofrecer bienes y servicios más competitivos? ¿No serán mejor gestionadas por algoritmos que por humanos formados en Administración de Negocios? [\[534\]](#)

2.6.1.1. El Caso TheDAO

Pero no todo lo que brilla es Oro. Es necesario en esta instancia volver a la realidad del mundo no digital, formado por seres humanos, muchos de los cuales se relacionan de un modo ético, y otros tantos, no.

TheDAO fue la primera DAO en ser testada en el mundo digital. La historia no tiene un final feliz, pero al menos nos demuestra que es posible dar vida a una DAO. Los hechos del caso fueron los siguientes:

1. *TheDAO* fue una DAO, es decir, una organización virtual [\[535\]](#), creada por una empresa alemana, Slock.it [\[536\]](#) en la *blockchain* de Ethereum. La Securities and Exchange Commission de EE.UU (SEC) definió los siguientes aspectos sobresalientes:

“The DAO was created by Slock.it and Slock.it’s co-founders, with the objective of operating as a for-profit entity that would create and hold a corpus of assets through the sale of DAO Tokens to **investors**, which assets would then be used to fund “projects.” The holders of DAO Tokens stood to share in the anticipated earnings from these projects as a return on their investment in DAO Tokens. A DAO Token granted the DAO Token holder certain **voting and ownership rights**. According to promotional materials, The DAO would earn profits by funding projects that would provide DAO Token holders a return on investment. DAO Token holders would then vote to either use the rewards to fund new projects or to distribute the ETH to DAO Token holders. In addition, DAO Token holders could monetize their investments in DAO Tokens by re-selling DAO Tokens on a number of web-based platforms that supported secondary trading in the DAO Tokens. In addition to secondary market trading on the Platforms, after the Offering Period, DAO Tokens were to be freely transferable on the Ethereum Blockchain. DAO Token holders **would also be permitted to redeem their DAO Tokens** for ETH through a complicated, multi-week (approximately 46-day) process referred to as a DAO Entity “split.”

The DAO was to be “decentralized” in that it would allow for voting by investors holding DAO Tokens. All funds raised were to be held at an Ethereum Blockchain “address” associated with The DAO and DAO Token holders were to vote on contract proposals, **including proposals to The DAO to fund projects and distribute The DAO’s anticipated earnings from the projects it funded.**

The DAO was intended to be “autonomous” in that project proposals were in the form of Smart Contracts that exist on the Ethereum Blockchain and the votes were administered by the code of The DAO. Submitting a proposal to The DAO involved: (1) writing a Smart Contract, and then deploying and publishing it on the Ethereum Blockchain; and (2) posting details about the proposal on The DAO Website, including the

Ethereum Blockchain address of the deployed contract and a link to its source code. **Proposals could be viewed on The DAO Website as well as other publicly-accessible websites** (...) there were two prerequisites for submitting a proposal. An individual or entity must: (1) own at least one DAO Token; and (2) pay a deposit in the form of ETH that would be forfeited to the DAO Entity if the proposal was put up for a vote and failed to achieve a quorum of DAO Token holders.

ETH raised by The DAO was to be distributed to a Contractor to fund a proposal only on **a majority vote of DAO Token holders**. DAO Token holders were to cast **votes, which would be weighted by the number of tokens they controlled**, for or against the funding of a specific proposal. Before any proposal was put to a vote by DAO Token holders, it was required to be **reviewed by one or more of The DAO's "Curators."** At the time of the formation of The DAO, the Curators were a group of individuals chosen by Slock.it (...) Curator was responsible for: (1) confirming that any proposal for funding originated from **an identifiable person or organization**; and (2) confirming that **Smart Contracts associated with any such proposal properly reflected the code the Contractor claims to have deployed on the Ethereum Blockchain**. If a Curator determined that the proposal met these criteria, the Curator could add the proposal to the "whitelist," which was a list of Ethereum Blockchain addresses that could receive ETH from The DAO if the majority of DAO Token holders voted for the proposal.

The DAO Website (...) described how The DAO operated, and included a link through which DAO Tokens could be purchased. The DAO Website also included a link to the White Paper, which provided detailed information about a DAO Entity's structure and **its source code** and, together with The DAO Website, served as the primary source of promotional materials for The DAO. On The DAO Website and elsewhere, **Slock.it represented that The DAO's source code had been reviewed by "one of the world's leading security audit**

companies.” [\[537\]](#) (los resaltados son míos).

2. Los DAO Tokens fueron ofrecidos al público entre el 30/04/16 y el 28/05/16. Fue un éxito histórico de ventas: se vendieron 1.150 millones de DAO Tokens a unos 11.000 inversores, levantándose 12 millones de Ethers –equivalentes, a tal momento, a unos 150 millones de USD– en la campaña más grande y exitosa de crowdfunding de la historia [\[538\]](#).

3. Días antes de finalizar el *road show* de los DAO Tokens (i.e., 28/05/16) comenzaron a circular rumores de posibles errores de programación en el código de la DAO. El 25/05/16 los organizadores (i.e. Slock.it) propusieron establecer un mecanismo de recompensas para quien descubriera y denunciara fallas de seguridad en el código, pero la propuesta no fue aceptada por los inversores por considerarla muy cara (su costo era de 125.000 ETH, aproximadamente el 1% del total del patrimonio de *TheDAO*). El 26/05/16, los organizadores propusieron designar a un experto en seguridad para que auditara el código de *TheDAO* [\[539\]](#).

4. El 17 de Junio de 2016, una persona o grupo de personas no identificadas detectaron un *bug* [\[540\]](#) en el código de *TheDAO*, y lograron que 1/3 del total del patrimonio de *TheDAO* fuera transferido a otra cuenta en Ethereum, a donde quedó inmovilizado por 27 días [\[541\]](#). El 20 de Julio de 2016, por mayoría de nodos, se decidió implementar un muy debatido *hard fork* en la *blockchain* de Ethereum, que permitió que los fondos fueran enviados a una nueva cuenta, en la cual los inversores perjudicados podían cambiar sus DAO Tokens por Ether, y salir de *TheDAO* como si no hubieran sufrido ninguna pérdida. Una minoría que votó en contra del *hard fork* no actualizó el software a la nueva versión de Ethereum, por lo que al día de hoy existe una *blockchain* llamada Ethereum Classic (ETC), y una Ethereum post-*TheDAO* (ETH) [\[542\]](#).

Los términos y condiciones publicitados por *TheDAO* expresamente negaban que los DAO Tokens fueran participaciones sociales, acciones o títulos valores similares en ninguna persona jurídica en ninguna jurisdicción del mundo, por lo cual los inversores que los adquiriesen no eran socios [\[543\]](#). Sin embargo, la SEC afirmó que los DAO Tokens eran títulos valores sometidos a su competencia y jurisdicción [\[544\]](#), ya que había una promesa de ganancia derivada o producto de la gestión empresarial de *otras personas*. En contra de esta opinión de la SEC, se ha sostenido que en *TheDAO* eran los propios inversores los que decidían a dónde invertir; y no un equipo de gestión. No existían, de hecho, autoridades formales en *TheDAO* [\[545\]](#).

Recientemente, Laila Metjahic ha analizado el caso en profundidad en un muy interesante y jugoso artículo publicado en la prestigiosa CARDOZO LAW REVIEW [\[546\]](#) y “curado” por Aaron Wright. En los apartados siguientes se seguirá la exposición de Metjahic, quien identificó las siguientes cuestiones legales:

2.6.1.1.1. Responsabilidad de los inversores y desarrolladores

Afirma Metjahic que bajo la legislación societaria norteamericana, los inversores y desarrolladores de *TheDAO* podrían ser considerados socios de una *general partnership*, en la cual asumen responsabilidad directa, ilimitada y solidaria ante terceros, y ciertos deberes fiduciarios entre ellos [\[547\]](#).

En nuestro derecho, sería equiparable a la responsabilidad del socio colectivo, con la importante diferencia de que éste asume una responsabilidad subsidiaria y puede invocar el beneficio de excusión [\[548\]](#). También podría ser asimilada a la calidad de socio de una sociedad simple, regulada en la Sección IV de la Ley General de Sociedades, en la cual el socio asume frente a terceros una responsabilidad mancomunada y subsidiaria, en principio [\[549\]](#).

Metjahic también se pregunta si *TheDAO* podría ser considerada una

sociedad anónima ^[550], y responde negativamente, ya que no delegaron el poder de decisión en un órgano de administración, sino que gracias a la descentralización de la *blockchain*, retuvieron para sí el poder de decidir en qué negocios se invertiría el capital digital.

En nuestro derecho, en las sociedades por partes de interés –entre las que se incluye la sociedad colectiva, y a donde no hay limitación de la responsabilidad del socio– la sencilla estructura de las mismas no requiere la existencia de órganos diferenciados –como en el caso de las sociedades de capital, donde sí se limita la responsabilidad del socio–, adoptando un *auto-organicismo de estructura simple*, por cuanto el carácter de órgano corresponde a cualquier socio, que actúa de manera directa como si fuera la sociedad ^[551].

2.6.1.1.2. Naturaleza jurídica de la participación societaria

Como consecuencia del encuadre de *TheDAO* como *general partnership* bajo el derecho anglosajón, en opinión de Metjahic la participación de sus socios –llamada *partnership interests* en EE.UU; partes de interés en nuestro derecho ^[552] – encuadra dentro de la definición federal de *security* –título valor–. A la misma conclusión llegó la SEC al analizar la plataforma fáctica del caso *TheDAO*, citando el *holding* del año 1946 *in re SEC v. W.J. Howey, Co.* ^[553].

Como consecuencia de lo anterior, el ofrecimiento público de un *security* debe (i.e. debió) cumplir ciertas normas registrales previo a su ofrecimiento, bajo apercibimiento de acciones civiles y penales a ser iniciadas por la SEC ^[554] –que finalmente no se iniciaron ya que el *hard fork* de Ethereum volvió las cosas a su estado anterior, y no hubo perjuicios causados más allá de la desilusión general–.

2.6.1.1.3. Status legal de una DAO: una propuesta de lege ferenda

Afirma Metjahic que el diseño de *TheDAO* encuadraba (y en el futuro, encuadraría) en la definición de *general partnerships* ^[555], o, en su defecto, en la definición de joint venture, que para el derecho norteamericano es tratado en muchos casos como una general partnership con objeto específico ^[556].

En el Estado de Delaware, por ejemplo, la definición de Joint Venture pivotea sobre cinco elementos:

- i) debe existir una comunidad de intereses en el resultado de un negocio común;
- ii) debe haber control común de la empresa;
- iii) debe existir un derecho de propiedad compartido en relación al objeto o resultado de la empresa común; y
- iv) un interés compartido en repartir las ganancias y soportar las pérdidas ^[557]. Afirma Metjahic que *TheDAO* cumplía, con certeza, estos cinco requisitos.

Por otro lado, los tokens emitidos por *TheDAO*, en opinión de Metjahic eran (y, en el futuro, serían) *securities* según la legislación federal de títulos valores que la SEC debe hacer cumplir. Es más, afirma Metjahic que la SEC ya ha considerado en 2014 que bitcoin es un *security*, igual que Ether ^[558]; y que los tokens emitidos por *TheDAO*, pagados con Ether, eran un contrato de inversión ya que:

“..the DAO is a scheme whereby a person invests his money in a common enterprise and is led to expect profits solely **from the efforts of a third party**. As such, the DAO is an investment contract, **with Ether as the security interest**. Together, the DAO and its sale of Ether should be considered security interests subject to SEC regulation. ^[559]” (el resaltado es mío).

La opinión de Metjahic no se comparte, ya que en el esquema de *TheDAO*

no existía la figura del promotor de *Howey*; no existió un tercero ^[560] que realice o brinde esfuerzos manageriales para extraer una rentabilidad repartible; y de hecho, los propios tenedores de tokens eran quienes votaban dónde invertir el activo digital de *TheDAO*.

2.6.3. DAOs, DACs e Internet of Things

El potencial de las DAOs y DACs va de la mano del crecimiento de la *IoT* a nivel doméstico, e industrial –*Industrial Internet of Things: IIoT*–. En efecto, Christidis y Devetsikiotis ^[561] afirman que la tecnología descentralizada y *peer-to-peer* de la *blockchain* es ideal para el desarrollo y expansión del ecosistema de *IoT*, con grandes beneficios tanto para los productores de dispositivos, como para sus usuarios ^[562].

La combinación de *blockchain*, *Smart Contracts*, DAOs y *IoT* puede permitir diseñar e implementar ejemplos como el que sigue, que probablemente en poco tiempo será seguramente un caso real de uso: un Municipio X que decide adquirir 2.000 bicicletas para uso social y comunitario, repartidas en 100 estaciones barriales con 20 bicicletas cada una, con su respectivo chip RFID que le da conectividad permanente: *IoT*. Cada usuario que desee usar una bicicleta, debe descargar una app, acreditar su identidad con lectura del código de barra en su DNI, y cargar crédito, comprando BiciTokens, cuyo valor es fijado por el Municipio. Cada BiciToken permite circular 100 horas, en tramos de 1 hora cada uno. Los BiciTokens son para uso personal, pero pueden ser cedidos gratuitamente a otros usuarios de la red. Cada 100 horas de circulación en bicicleta, el sistema acredita 0.5 BiciTokens en la cuenta del usuario, como premio por ejercitarse y utilizar un medio de movilidad sustentable. Todo el sistema corre en una *blockchain* privada, permissionada, donde existen tres nodos:

- i) el Municipio: que vende o acredita los BiciTokens a los ciudadanos dados de alta;
- ii) un servicio de mantenimiento de las bicicletas, que pueden ser organizaciones sociales o centros vecinales, ya que se sabe que el 2% de ellas debe ser reparado mensualmente; y

iii) sponsors privados, que aportan fondos para adquirir las bicicletas y para mantener el sistema, y que pueden disparar campañas de marketing segmentadas para los usuarios.

Todo el sistema se programa para operar como una Organización Autónoma Decentralizada (DAO), es decir, un conjunto de contratos inteligentes que interactúan entre sí, y donde se configuran las siguientes funcionalidades:

(1) si un usuario acredita 1000 horas de movilidad sustentable –el sistema vía RFID lo puede confirmar–, el Municipio puede premiar tal conducta con beneficios fiscales –reducción del 1% en cualquier tasa municipal que el usuario deba pagar;

(2) si un usuario acredita la reparación de 10 bicicletas en un mes, certificadas por el servicio de mantenimiento, puede acceder a los mismos beneficios que en el caso anterior;

(3) los sponsor privados pueden comprar publicidad estática en las 100 estaciones y en las 2000 bicicletas móviles así como banners en la app, sea entregando nuevas bicicletas al sistema, reparando las afectadas, o acreditando beneficios –vouchers, descuentos, canjes– para los usuarios del sistema, bajo forma de BiciTokens con afectación específica –por ejemplo, el pago de restaurants, vestimenta, etc. –, permitiendo el sistema segmentar y premiar a los más comprometidos (e.g., los que pedalean más de 500/1000/2000 horas mensuales);

(4) las compras de publicidad estática o móvil por parte de privados puede, a nivel del usuario, ser reflejada en contratos inteligentes que le permiten acceder automáticamente a los beneficios sólo si se cumplen determinadas condiciones –e.g., pedalear 3000 horas–, y estos beneficios pueden ser cesibles, o de uso personal, según cómo se configure el contrato inteligente que los aloja; y

(5) al estar registrado en una *blockchain*, el funcionamiento del sistema es transparente, auditable, y medible desde el punto de vista de mitigación del Cambio Climático.

Una DAO como la expuesta, no tiene fines de lucro, sino un fin muy distinto: promover la movilidad sustentable y crear un circuito cerrado –pero auditable y transparente– de premios e incentivos públicos y privados para una Ciudad Sostenible. Una DAO como la expuesta es una entidad digital que funcionará del modo que se la programe, sin necesidad de intervención humana, pudiendo incluso pagar los servicios *off-chain* de mantenimiento brindados por el nodo de mantenimiento mediante una moneda nativa, BiciRepairToken, que sea canjeable por moneda de curso legal, a donde los privados pueden comprar BiciRepairTokens de modo tal que los reparadores cobran por su trabajo, también mediante contratos inteligentes. Todos los tokens del sistema se representan en códigos QR, que son escaneados desde aplicaciones móviles, con lo cual sólo se requieren Smart Phones, cada vez más frecuentes.

Ahora bien, para finalizar, se ha sostenido que la autonomía completa de un *Smart Contract* puede ser una espada de doble filo [\[563\]](#), y deben tomarse recaudos a nivel de arquitectura de software que permitan modificar los outputs de un contrato inteligente en función de distintos inputs variables, o que permitan directamente eliminar el contrato de la *blockchain* mediante una función de “auto-destrucción” [\[564\]](#). De lo contrario, el sistema –i.e. la DAO– no podría ser modificado y es posible imaginar casos donde tokens o monedas sean retenidas *ad infinitum* por un error de programación. Un contrato inteligente que retenga lo que, por alguna razón, debe ser liberado, debe poder ser eliminado.

2.6.3. Round 2: Enter The LAO (DAOs 2.0!)

Como se dijo más arriba, la década de 2020-2030 será la *Década de las DAOs*, y el debut accidentado del *TheDAO* no podrá detenerlo. Así, a fines de 2019 ya se ha propuesto una nueva estructura, bajo la creencia firme de que las DAOs tienen el (enorme, por cierto) potencial de reducir costos de transacción al confiar y delegar en contratos inteligentes el gobierno y la coordinación de acciones y comportamientos on line [\[565\]](#). La tesis subyacente es simple, y puede dar nacimiento al Gobierno Corporativo 2.0:

“Through the use of Smart Contracts, parties can automate certain aspects related to the way organizations and groups operate, reducing operational costs and improving internal controls while simultaneously increasing the overall transparency of an organization. [\[566\]](#)”

A continuación se resaltan los caracteres más sobresalientes de esta nueva e interesante figura legal digital que se propone:

“The LAO will provide a legal structure to enable members to not just give grants, but to invest in blockchain-based projects in exchange for tokenized stock or utility tokens. Projects or Ethereum-based projects will be able to receive funding for their projects in days once submitted to the LAO.

Using the tooling provided by OpenLaw, **the LAO will be set up as a limited liability entity, organized in Delaware, using curated [Smart Contracts](#) to handle mechanics related to voting, funding, and allocation of collected funds.** This entity will presumably limit the liability of LAO members and help clarify their relationship to avoid knotty questions related as to whether partnership law applies.

This structure will also provide members of the LAO with tax flow — through treatment by the Internal Revenue Service, such that tax is not paid by both the entity and a person holding a beneficial interest in the LAO.

Members will be able to purchase interests in the LAO and the proceeds from the purchase will be pooled and allocated by members to startups and other projects in need of financing, using a voting mechanism and tools similar to Moloch DAO.

In order to comply with United States law, **membership interests of the LAO will be limited and only available to parties that meet the definition of an accredited investor —**

although there are arguments that LAO membership interests may not be securities. And, the LAO will be anchored by 10 founding members (which will be announced shortly). Other interested parties will be able to purchase interests in the LAO (potentially through a public sale).

Through OpenLaw's tools, the creation and set up of The LAO will be streamlined. **All of the relevant legal documents from the entity formation documents to member subscription agreements will be generated via the OpenLaw protocol** — taking complex corporate financial processes and streamlining their operation — while also providing members with the backing of the U.S. legal system. We also will be exploring on-chain verification of accredited status for the LAO using third-party oracle services (such as [ChainLink](#)) to streamline the onboarding process.

Much like the original Moloch design, **members of the LAO will be able to ragequit and immediately retrieve back their fair share of unallocated funds based on their economic contribution (regardless of voting weight)**. With this safety mechanism in place, **LAO members will always have the option to opt-out of the LAO should they disagree with aspects of the LAO membership, investment portfolio or need to rapidly receive back their assets**. Extending emerging Moloch designs further, LAO members can also continuously claim their fair share of profits provided by tokens received from projects that receive investment from the LAO, further incentivizing collective LAO diligence, voting participation, and membership stability.

The LAO will allocate to potential projects funding in Ether (or potentially DAI). **Funding will be provided once a member nominates a project for funding and a majority of the members (based on their voting weight) approve the allocation of funds**.

The funding will be provided on a take it or leave it basis. **The LAO will receive a certain portion of the projects tokenized stock or other ERC-20 token in exchange for a fixed amount**

of funding from the LAO.

To accept funding, projects will submit an application and be **required to create a Delaware legal entity and OpenLaw will provide a set of standardized documents to streamline the process.** If the project is later stage, OpenLaw will work with the project to ensure that the LAO can provide funding, given the project or entity's then-current legal structure.” [\[567\]](#) (los resaltados son míos)

Sin dudas, con la muy reciente irrupción del *LAO* estamos frente a un concepto que al final de la década habrá disruptado al derecho societario, al menos en lo que a negocios digitales se refiere. La ola de las DAOs 2.0 ya inició, y mientras estas líneas se escriben, se escriben también las líneas de programación del *TheDAO reloaded* [\[568\]](#). Como se dijo antes, durante esta década se verán nuevos desarrollos a medida que madure la *Blockchain* 2.0 hacia una *Blockchain* 3.0.

2.6.3.1. *Ragequit, o el derecho de receso digital en el Siglo XXI*

Antes de finalizar este tratamiento superficial de las DAOs y las LAOs, quiero volver a llamar la atención sobre un concepto que, como profesor de Sociedades, luce muy interesante, y hasta familiar: *Ragequit*, una función desarrollada en los contratos inteligentes que ofrece una DAO llamada *MolochDAO* [\[569\]](#), descrita en su White Paper en los siguientes términos:

“We recognize that in any voting-based system, there are a large number of edge cases created by possible collusion or unavailability of stakeholders. To handle these, **we built a catch-all mechanism that allows participants to exit with their funds if they did not agree with the result of a vote.** This is done by allowing members to “Ragequit” the guild **within a “grace period” after voting on a proposal completes but before those members’ ownership is affected by that**

proposal.

Let's say for instance that 99% of the guild colludes and submits a proposal to issue 99% more Shares to themselves and dilute the remaining 1% down to effectively zero. In this case, the 1% would Ragequit the guild during the grace period, negating the majority voting bloc's attack.

Note that the remaining members after the grace period ends bear the cost of the proposal. **In the case of a contentious vote where a large minority exits (e.g. a 51% attack), this means that cost is greatly increased for those who stay.** To enforce this, we restrict Ragequitting to only members who voted "No" in a given proposal if the proposal passes. This forces "Yes" voters to bear the cost of a malicious proposal.

We expect this to create an interesting additional meta-incentive for mutual cooperation, since **guild members would be strongly disincentivized to submit proposals that might cause a large proportion of other members to ragequit.**

Readers may note that an attack vector exists where participants can repeatedly Ragequit to either avoid dilution or grief the guild. This would be an effective method to avoid paying the cost of a single proposal. However, if the member wanted to avoid paying they would have to Ragequit the entirety of their shares, completely removing them from the guild. They would then have to reapply as a member, and we expect that existing members would be hesitant to readmit the defecting applicant. From existing game theoretic research, we are confident that this will be a strong incentive for members to not abuse the ragequit mechanism. ^[570] (los resultados son mios)

Si uno entiende el funcionamiento de la función *ragequit*, y conoce el funcionamiento del derecho de receso en materia societaria ^[571], encontrará llamativas similitudes y muchos puntos de contacto.

2.7. *Haciendo marcha atrás con un Smart Contract: ¿Se puede?*

Habiendo visto hasta ahora las muchas definiciones de un contrato inteligente, sus distintas clasificaciones posibles, sus cuatro pilares fundamentales, algunos casos de usos y muchos de los problemas asociados a ellos, la pregunta que ahora debe estar en el aire es: si un contrato inteligente funciona mal, por acción u omisión de su programador ¿es posible volver hacia atrás, sin tener que impulsar un *hard fork* y romper la inmutabilidad de la *blockchain*, tal como ocurrió en el caso *TheDAO*?

Evidentemente, la cuestión tiene distinta naturaleza (y posibilidad de respuesta) en *blockchains* públicas que en *blockchains* privadas o consorciadas. En éstas, la arquitectura puede prever formas de retrotraer los efectos de un contrato inteligente, ya que en alguna medida, hay un control central.

Por el contrario, en *blockchains* públicas, especialmente en Ethereum, la cuestión aún no tiene una respuesta clara, y quizás haya que esperar hasta tener una respuesta o técnica sólida. De allí la imperiosa necesidad de *auditar* el código del contrato inteligente antes de que sea puesto en acción, necesidad que tiene una cada vez mayor oferta de servicios [\[572\]](#), y que será analizado en profundidad en el Capítulo IV.

2.7.1. *Token propio*

Se ha sostenido que una posibilidad de “dar marcha atrás” depende de que el token en cuestión sea un token propio del proyecto o de la empresa fondeada. En éstos casos, es posible retrotraer operaciones; o bien congelar los tokens afectados y emitir nuevos en su reemplazo [\[573\]](#), pero evidentemente requieren un “control central” que está en las antípodas de la descentralización que plantea la *blockchain*.

2.7.2. *¿Contrato reversible?*

Se ha señalado que *existen* formas de “actualizar” un *Smart Contract* que no está funcionando correctamente o tiene alguna vulnerabilidad detectada, sin que ello implique *ipso facto* poder revertir las operaciones defectuosas [\[574\]](#). Así, una forma es crear un contrato intermedio –i.e. *caller contract*–, que aloja la dirección del contrato activo o principal –i.e., *target contract*– [\[575\]](#).

2.8. Hacia la estandarización de Smart Contracts

Como se verá más abajo en § 3.4.1.3, el Reino Unido recientemente ha considerado que los criptoactivos son una propiedad tranzable y que los *Smart Contracts* son contratos válidamente celebrados bajo la legislación inglesa [\[576\]](#).

En la misma línea, recientemente, el BRITISH STANDARDS INSTITUTE ha iniciado un proceso de elaboración participativa de estándares para *Smart Contracts* [\[577\]](#), enfocándose en las especificaciones técnicas que debieran cumplir los contratos que sean legibles tanto por humanos como por máquinas, con el fin de fijar un estándar para toda la industria que se dedica al desarrollo de software que utiliza, ofrece o codifica *Smart Contracts*, tanto actuales como futuros [\[578\]](#).

Vinculado a la estandarización [\[579\]](#), en un muy interesante trabajo del año 2016, Clack, Bakshi y Braine [\[580\]](#) indagan en la conveniencia de generar *modelos* de *Smart Contracts* para redes descentralizadas, con la mira puesta en la industria de las finanzas, y con el objetivo de facilitar el cumplimiento automático y que, en caso de conflicto, tengan una referencia a la documentación legal subyacente [\[581\]](#).

Estos modelos estandarizados de *Smart Contracts* utilizan parámetros que conectan el lenguaje natural legal –la prosa legal [\[582\]](#)– con su correspondiente lenguaje de programación *machine-readable*. Dichos parámetros operacionales permiten direccionar el comportamiento del *Smart*

Contract^[583], pero determinarlos puede no ser tan sencillo^[584]. Concluyen los autores afirmando que el uso de parámetros no solo agilizaría la estandarización del lenguaje de programación para *Smart Contracts*, sino que también produciría que en el futuro, la prosa legal se exprese de forma más estructurada y formal, e incluso, hasta permita reemplazar la lógica a veces ambigua de la prosa legal por expresiones aritméticas y lógicas, lo que a su turno reduciría la ambigüedad y los errores en el lenguaje natural legal^[585].

A su vez, mientras más estandarizado sea el código de los *Smart Contracts*, lo vuelve más genérico, y en algún punto se llegaría a un código de programación compartido, común, y de uso masivo^[586].

III. Tokens & *Smart Contracts* vs. La Ley

3.1. La declaración de independencia del Ciberespacio

El 8 de Febrero de 1996, John Perry Barlow, activista digital de la ELECTRONIC FRONTIER FOUNDATION^[587], pronunció la *Declaración de Independencia del Ciberespacio*^[588], y en términos muy enfáticos, afirmó allí que no existe soberanía estatal alguna en el ciberespacio:

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. **You have no sovereignty where we gather.**” (el resaltado es mío)

Tan osada afirmación encendió por aquél momento un debate global muy intenso cuando la Internet 1.0 –la Internet comercial o *Internet de la Información*– comenzaba a dar sus primeros pasos. Como se adelantó en el Capítulo I, la batalla parecía inevitable, entre dos bandos muy claros: los ciberlibertarios, por un lado, que promovían la innovación (digital), y que afirmaban que la naturaleza distribuida y global de Internet la volvían ingobernable por los Estados, colocándola fuera del alcance de la Ley, debido principalmente al anonimato que Internet permite y a la gran movilidad de los participantes en el ciberespacio, pudiendo “relocalizarse” libremente dentro del ciberespacio^[589].

Por otro lado, emergieron (antes y ahora) los ciberpaternalistas, sosteniendo la procedencia de la regulación estatal, afirmando que nada intrínseco a la naturaleza de Internet (o de la *blockchain*, hoy) la eximía de cumplir las Leyes o de liberarse del Estado de Derecho. En aquél momento, Lessig afirmó que las leyes ordinarias que rigen las conductas en el mundo real regulaban también la conducta en el ciberespacio, aunque la eficacia de este control dependía de las características del ciberespacio, pudiendo los

Estados regular el código –i.e. programación– en sí, y a los programadores que programan el contorno del ciberespacio.

Como ya se apuntó antes ^[590], el tiempo le dio la razón a los ciberpaternalistas, y la pregunta que la *Internet del Valor* hace (nuevamente) surgir, es si los Estados podrán (o deberán) controlar su desarrollo y expansión, del mismo modo en que lo hicieron con la *Internet de la Información*.

Siguiendo a Lessig ^[591], se sostiene que la *blockchain*, su ecosistema y la Internet 3.0, la *Internet del Valor* ^[592], dentro de la cual se incluye a la criptoconomía, las CBDCs, la tokenización de variados tipos de activos y a los contratos inteligentes, pero también otras formas de digitalización de la Economía combinando *IoT*, *IIoT* y sistemas expertos de *Machine Learning* aplicado, *necesitará* a las Leyes y a los Estados (regulaciones), para hacer cumplir contratos “implícitos” y cláusulas no explícitas (i.e., no programadas), y para gestionar también eventuales contingencias que se produzcan por eventos previsible pero inevitables, como lo son los ciberataques.

Sin embargo, los defensores más agresivos de la *blockchain* auguran una masiva desintermediación multi-sectorial, y pregonan la posibilidad real de crear comunidades digitales con reglas propias, pudiendo incluso crear nuevas entidades gubernamentales.

Wright y De Filippi lo exponen en estos términos:

“...through the deployment of increasingly complex systems of Smart Contracts and decentralized organizations, the technology can be used to **establish rules and structures for organizations, formal entities, and potentially even governmental bodies**. If designed to capture human input, the technology can be used to reflect community values and social norms, automatically enforced through self-executing code. Smart Contracts may even re-write or bypass some of the most basic tenets of property law, **effectively turning property or**

even constitutional rights into a subset of contract law. Judicial enforcement of law could also be displaced by blockchain technology. Smart Contracts can be made to rely on a certain degree of human judgment at any point during the contract's execution. For instance, in order to determine whether or not certain contractual conditions have been met, contractual conditions could be made dependent on the judgment of one or more external parties (so-called "Oracles"). Of course, one of these parties could be the judiciary, but it could also be a panel of independent arbitrators, or a jury summoned from around the Internet, selected and paid based on their track record of deciding earlier disputes. [\[593\]](#)," (el resaltado es mío)

En la vereda de enfrente, Werbach afirma que, tal como ya se vió en los últimos 20 años, los gobiernos y las poderosas corporaciones privadas no se dejarán *desintermediar* tan fácilmente [\[594\]](#), y lo pone en estos términos:

"Where they had a strong desire to regulate online activity, they found ways to do so. A similar pattern seems likely for activity on the blockchain: **Where the stakes are high enough, governments will not simply defer their authority.** Even when transactions are entirely digital, peer-to-peer, cross-border, and cryptographically secured, **providers on the network can be identified and subject to territorial legal obligations.** Moreover, outside of activity that is illegal or in need of extreme security, the incentives are lacking for most users to adopt custom legal systems where the existing ones are functional. **And as the creators of The DAO discovered, taking the place of law is not as easy as it may seem.** [\[595\]](#)," (el resaltado es mío)

En la misma línea, también se ha sostenido que:

“Bitcoin fails to embody any substantial alternative to [our existing financial systems]. The reasons for this have little to do with technology and everything to do with the financial systems in which Bitcoin and all other cryptocurrencies are embedded, systems that instantiate the **forms of power that cannot be eliminated through either wishful thinking or technical or even political evasion: the rich and powerful will not become poor and powerless simply because some people decide to operate alternative exchange economies.** Lacking a robust account of transforming these systems of power, even without Bitcoin’s flaws, a ‘perfect’ cryptocurrency would exacerbate, rather than address, the existing serious problems with our monetary and financial systems” [\[596\]](#) (el resaltado es mío)

Werbach reconoce que muchos creen y afirman que la regulación estatal de la criptoeconomía en general, y de los sistemas del entorno *blockchain* en particular, no sólo corromperá el proceso sino que lo hará ir más lento [\[597\]](#), pero Werbach rebate con altura el punto, afirmando enfáticamente que la regulación de Internet fue lo que permitió su adopción masiva [\[598\]](#), y ejemplifica con la intervención antitrust en EE.UU contra Microsoft, en resguardo de la competencia en entornos digitales. Las detenciones de Ross Ulbricht [\[599\]](#) y de Alexander Vinnik [\[600\]](#) demuestran que las regulaciones (y las sanciones) pueden penetrar en el entorno *blockchain*.

Es entonces evidente que la tecnología digital del mundo contemporáneo es una espada de doble filo, que puede ser usada para el bien, y para el mal [\[601\]](#). La historia no es nueva; *blockchain* es sólo un *capítulo* nuevo. Y, sin dudas, los países que voluntariamente decidan no hacer nada al respecto y desentenderse del tema, serán una mayor amenaza para el desarrollo del ecosistema *blockchain* que aquéllos otros que estudien el fenómeno, comprendan sus virtudes, conozcan sus defectos e intenten regular su desarrollo de manera acorde [\[602\]](#). Como con gran claridad sostiene Gustavo

Bélic respecto de la Inteligencia Artificial, “*todo esfuerzo que apunte a reducir los obstáculos al comercio y facilitar la internacionalización de nuestras empresas –con particular énfasis de las pequeñas y medianas de la base de la pirámide– será un paso en la dirección adecuada. En esta tarea, la IA –mutatis mutandis, la blockchain– ya no debe ser vista como una opción, sino como una obligación. La amenaza inmediata no es la aplicación de la IA –mutatis mutandis, la blockchain–, sino su menosprecio.*” [\[603\]](#)”

Ante este panorama que parece una *vuelta al pasado*, se vuelve a sostener hoy que tal dicotomía (innovación vs. regulación; tokens y *Smart Contracts* vs. the Law) no debiera ni existir, y es importante que no se pierda tiempo en discutir lo que no existe. La realidad, innegable, es que el Estado y los Gobiernos tienen un gran potencial para ser los primeros facilitadores de la innovación, verdaderos *early adopters*. El verdadero (y muy complicado) desafío es *educar* a los que toman las decisiones desde el sector público, los *policy makers*, para que no tomen medidas que puedan inhibir o diferir la innovación.

Con tal perspectiva, en este capítulo se pasará revista al estado actual comparado de cómo las legislaciones estatales comienzan a abordar el nuevo fenómeno de los criptoactivos y los contratos inteligentes, y qué herramientas existen para delinear un campo de innovación controlada. Finalmente, se analizará la legislación argentina y cómo ésta puede receptor los nuevos conceptos de criptoactivos y contratos inteligentes y gestionar situaciones donde pueden darse conflictos, en especial respecto de consumidores y usuarios en caso de insolvencia, y en cómo defender la defensa de la competencia en entornos digitales.

3.2. Tres (posibles) formas de interacción entre la Blockchain y el Derecho

Antes de analizar distintos enfoques legislativos comparados, es conveniente estructurar analíticamente los posibles escenarios de *diálogo* entre la innovación y la regulación, entre la *blockchain* y el sistema legal. Para ello, se seguirá la muy interesante propuesta metodológica de Yeung [\[604\]](#),

que propone tres escenarios de interacción: evasión hostil, alineación eficiente y alivio de fricciones transaccionales.

3.2.1. Evasión hostil

En este escenario, el ecosistema *blockchain* es utilizado para evadir limitaciones sustantivas creadas por el régimen legal aplicable, y de manera directa y frontal cuestiona el Estado de Derecho sobre el cual se cimentan los países y sus soberanías. En estos casos, es esperable la reacción estatal, ya que la inacción produciría daños irreparables a posibles víctimas y afectaría gravemente la reputación de los órganos de regulación afectados, i.e. circunvenidos mediante el recurso a la cadena de bloques [\[605\]](#).

Yeung lo explica en los siguientes términos:

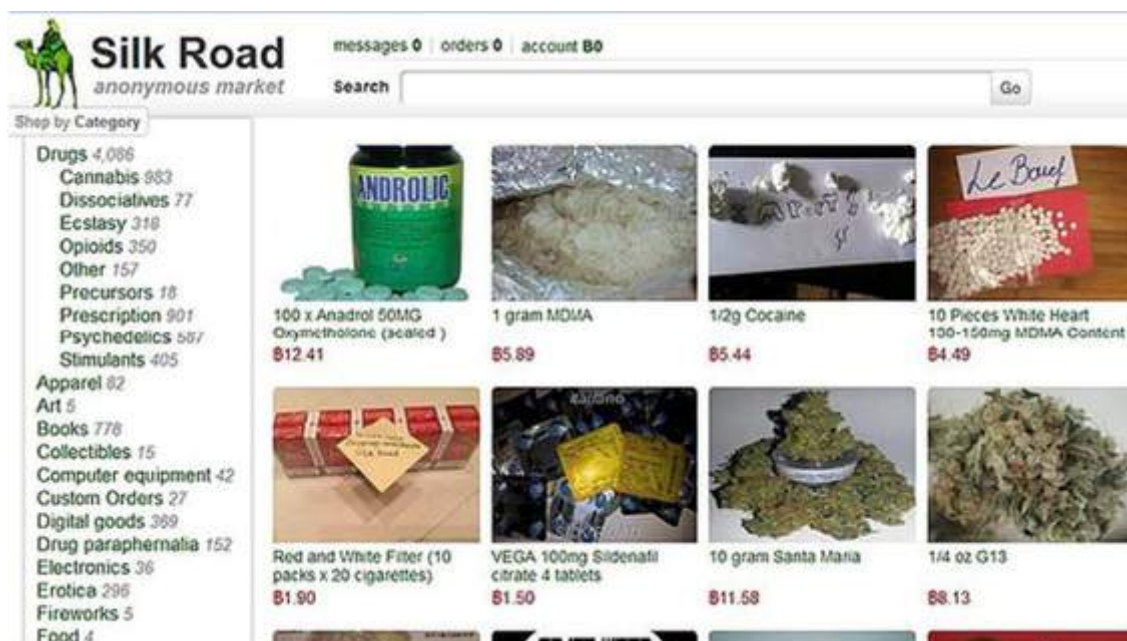
“We can therefore anticipate an active ‘battle for supremacy’ in which the **code of law attempts to assert its sovereign authority over code as law** to close off opportunities for actors to exploit the anonymised interactions which public blockchains make possible. This battle is unlikely, however, to take the form of a single, monumental winner-take-all ‘fight for survival’; more likely is a series of **on-going ‘cat and mouse’ interactions in which national legal authorities seek to close off loop-holes** that some blockchain users attempt to exploit to evade the law’s substantive demands. [\[606\]](#)” (El resaltado es mío)

Un ejemplo de este escenario es la utilización de criptomonedas con un velo de anonimidad para actividades ilegales –el célebre caso *SilkRoad*–, y otro ejemplo es Ripple, el primer *Exchange* en ser objeto y blanco de reacción estatal. En ambos casos, el patrón ha sido apuntar al intermediario [\[607\]](#), y no tanto a los usuarios o a la tecnología *blockchain* en sí, ni tampoco prohibir el uso de criptomonedas, lo que también será analizado más abajo.

3.2.1.1. SilkRoad

SilkRoad^[608] era un *marketplace* creado por Ross Ulbricht donde era posible comprar productos ilegales pagando con bitcoins. Fue el primer marketplace en aceptar bitcoin como medio de pago.

Imagen 11 SilkRoad



SilkRoad operó por casi 3 años desde 2010 a 2013, e intermedió 1.5 millones de transacciones en bitcoins por valor de 1.200 millones de Dólares^[609], cobrando una comisión del 10%. El explosivo crecimiento del portal se debe a que ofrecía un modo seguro y eficiente para adquirir productos que, en la vida real, son inseguros. Creó un sistema de reputación y rating de vendedores de productos ilegales, similar al de cualquier *marketplace* legal, garantizando que un vendedor que no cumpliera los estándares de calidad, sería eliminado de la red. Como plataforma, tuvo una tasa de crecimiento mayor a la de Uber, AirBnB o eBay^[610].

En 2015, Ross Ulbricht, el fundador de *SilkRoad*, con tan solo 31 años de edad fue condenado a dos cadenas perpetuas [\[611\]](#), y le fueron incautados 144.000 bitcoins.

3.2.1.2. Ripple

Ripple es a la vez una plataforma y una criptomoneda, XRP [\[612\]](#). Como plataforma, permite a través de RippleNet que cualquier persona cree su propia moneda y funciona también como *Exchange*. RippleNet, con una agresiva política de bajas comisiones, disruptó el mercado de transferencias internacionales, un mercado formado por 11.000 bancos de todo el mundo, hasta entonces servido sólo por la *Society for Worldwide Interbank Financial Telecommunication*, SWIFT [\[613\]](#), quien recientemente comenzó a probar la tecnología *blockchain* que ofrece Ripple [\[614\]](#).

En 2017, el Departamento del Tesoro de EE.UU, a través de FinCEN (“Financial Crimes Enforcement Network”) multó a Ripple en USD 700.000 por actuar como un *money services business* y vender su moneda XRP sin haberse previamente registrado en FinCEN, y además no implementar controles de *Anti-Money Laundering* (AML) y de *Know Your Customer* (KYC) en su plataforma [\[615\]](#). Simultáneamente, una acción penal fue suspendida a cambio de pagar una multa de USD 450.000 adicionales [\[616\]](#). En el momento, se declaró desde FinCEN lo siguiente:

“Ripple Labs Inc. and its wholly-owned subsidiary both have acknowledged that **digital currency providers have an obligation not only to refrain from illegal activity, but also to ensure they are not profiting by creating products that allow would-be criminals to avoid detection.** We hope that this sets an industry standard in the important new space of digital currency (...) Federal laws that regulate the reporting of financial transactions are in place to detect and stop illegal

activities, including those in the virtual currency arena (...) Unregulated, virtual currency opens the door for criminals to anonymously conduct illegal activities online, eroding our financial systems and creating a **Wild West environment where following the law is a choice rather than a requirement.** ^[617]” (el resaltado es mío).

3.2.1.3. La regulación de China sobre Bitcoin y blockchain

Como ya se puntualizó antes ^[618], China controla el minado de bitcoins pero ha prohibido el *Exchange* de criptomonedas desde 2017 ^[619] y, desde 2018, se prohibieron también las plataformas de *trading* que comercializan criptomonedas.

Pero los signos de los tiempos parecen estar cambiando en Asia, rápidamente. China ahora está decidida a liderar en la tecnología *blockchain*. Así, se avizora un cambio de enfoque ya que desde el 1 de Enero de 2020, rige una ley ^[620] que regula el uso de la criptografía con fines comerciales, con el fin de impulsar la investigación, la educación de la comunidad y su aplicación. La legislación clasifica la criptografía en *core*, ordinaria y comercial y estipula determinados requisitos que deben cumplirse si el uso de la tecnología puede afectar el interés general o secretos de estado ^[621].

3.2.2. Alineación eficiente

Yeung propone un segundo escenario, en el cual la *blockchain* es usada para dar soporte y eficientizar el cumplimiento de las normas vigentes ^[622]. Este uso puntual de la *blockchain*, alineado y/o al servicio del sistema legal aplicable, suele ser denominado Regulatory Technology, o *RegTech*, y se expresa en esta tesis:

“...public regulatory influence could be exerted through a

combination of legal and technical code, rather than through legal code as at present. In essence, **technical code could be used to assure compliance with legal code, and in so doing, reduce the costs of legal compliance.** This could provide a ‘use case’ for the use of technology to enhance regulation, so-called RegTech (...) any technological innovation that can be applied to or used in regulation, typically to improve efficiency and transparency.”^[623] (el resaltado es mio)

Ejemplos de este enfoque win-win se exponen a continuación.

3.2.2.1. Corda (R3)

Corda es una plataforma de registro descentralizado –i.e., una DLT, pero que no utiliza cadena de bloques– utilizada por 300 entidades financieras, entre ellas los bancos JP Morgan, Credit Suisse, UBS, Deutsche Bank, Barclays, reguladores^[624], bancos centrales y cámaras empresarias de primera línea, para gestionar y sincronizar los contratos y la documentación legal que fluye entre ellos^[625]. La plataforma es privada y permissionada, y utiliza *Smart Contracts* que son o refieren en todos los casos a contratos reales con efecto legal vinculante; recurre a distintos mecanismos de consenso para acordar sobre transacciones determinadas; no sobre el estado general de todo el registro –a diferencia de las *blockchains* públicas–.

Cada transacción en la plataforma es un contrato, y su información se comparte sólo entre las partes que tengan la vinculación contractual. No existe un registro central de todas las transacciones, sino que las partes que participan de Corda tienen sus propios registros, pero en lugar de centralizarlos en sus respectivo servidores, lo decentralizan mediante la plataforma, lo que facilita sobremanera el proceso de conciliación y reconciliación bancaria. Una figura llamada *notario* es la que garantiza que las transacciones sean correctas; y los notarios pueden competir entre sí para notarizar transacciones en la plataforma^[626].

Como plataforma, Corda permite además el desarrollo *sobre ella* de distintas aplicaciones, como la recientemente testada Voltron, en la cual participan 50 bancos de 27 países, y que busca simplificar la gestión de las cartas de crédito internacional, reduciendo procesos manuales de 10 días a 24 horas [\[627\]](#). Asimismo, Corda permite que ciertos reguladores tengan acceso en tiempo real a la información sobre transacciones que tienen lugar entre las partes de la plataforma, lo cual marca el carácter *RegTech* de la plataforma. Señala Yeung que Corda es un claro ejemplo de la DLT al servicio del régimen legal aplicable [\[628\]](#).

3.2.2.2. *Suplementar, complementar o sustituir*

En línea con el pensamiento de Yeung, Werbach [\[629\]](#) afirma que la posibilidad de que los reguladores sean nodos de una plataforma facilita la supervisión, en lugar de excluirla, como ilustra el caso de Corda. En estos casos, la DLT *suplementa* a la actividad de control y regulación.

En otros supuestos, la *blockchain* puede *complementar* los sistemas legales de control en casos en los que no funcionan de manera eficiente, como con las obras huérfanas [\[630\]](#). También en casos en los que ciertos intermediarios se quedan con la mayor parte del negocio, como ocurre con la industria de la distribución musical. La *blockchain* puede permitir formas de auto-gestión en la distribución digital de derechos, empoderando a los creadores, al conectarlos de modo directo con sus consumidores. Ejemplos de este enfoque son Ujo Music y la Open Music Initiative [\[631\]](#).

El caso de UJO Music es muy interesante: propone crear un ecosistema *on-chain* de artistas musicales descentralizado, donde los oyentes se conecten directamente con sus artistas, sin intermediarios [\[632\]](#). Corriendo sobre Ethereum, la plataforma –con una versión web y otra mobile– utiliza *Smart Contracts* para gestionar el licenciamiento de canciones, el pago, e incluyen un token propio, que denominan *Badges*, y que permiten comprar música y conectar de manera directa al artista con sus seguidores. UJO permite que los artistas suban sus obras a Ethereum, y puedan venderla en Ether; sus oyentes

también pueden adquirir *cryptocollectibles* ^[633] de sus artistas.

Finalmente, existen casos en los que la *blockchain* puede *sustituir* la forma tradicional, menos eficiente, de almacenar información y transaccionarla. Este es el caso de las *fintechs* que apuntan a la población no bancarizada, y también el de las cadenas de suministro con trazabilidad *on-chain* ^[634]. Y es también el caso de los registros inmobiliarios, afirmando el Banco Mundial que el 70% de la población mundial no tiene acceso a un título dominial correctamente registrado, y solo 1/3 de los países tienen registros digitales ^[635]. Los casos piloto de registro inmobiliario *on-chain* implementados en Georgia y también en Brasil ^[636], que también utiliza *blockchain* para registrar los nacimientos ^[637], son pasos firmes en esta dirección, en donde la *blockchain* representa (o puede representar) una mejora en la forma de hacer las cosas. Se volverá sobre estos y otros ejemplos de casos de uso en el Capítulo VIII.

3.2.3. Aliviar fricciones transaccionales

Un tercer escenario de interacción entre *Blockchain* y el Derecho que vislumbra Yeung ^[638] es aquél intermedio entre los dos anteriores, donde la tecnología se utiliza para diseñar nuevas formas de cooperación, más eficientes en términos de costos, barreras a la entrada y formalidades.

En estos casos, el sistema legal aplicable asumirá una posición de cautela. Señala la autora citada que la raíz fundacional de Bitcoin fue el fuerte descreimiento hacia el sistema financiero por la crisis de 2008, más allá de que años después se pagara la compra de sustancias ilegales con bitcoins en *SilkRoad*, o se la use como moneda de pago en ataques del tipo *ransomware* en la actualidad ^[639].

Con esa misma lógica, la *blockchain* ha sido también utilizada para diseñar, entre otras, nuevas formas de fondeo para nuevas empresas mediante Initial Coin Offerings, y nuevas formas de intercambio de energía, apalancando el mercado de generación eléctrica domiciliar o distribuida. Estos son,

entonces, ejemplos en los que la *blockchain* alivia fricciones transaccionales, permitiendo nuevas formas de organizar y realizar acciones de cooperación de un modo más eficiente vis à vis la forma tradicional de hacer las cosas.

3.2.3.1. Crowdfunding vía ICOs, STOs, DAICOs & IEOs. Reenvío a taxonomía del Token.

Antes que nada, debe precisarse que existen muchas tipologías de tokens o *appcoins*, lo que se analizará en profundidad más abajo en § 3.3.1 [640]. Genéricamente, las ventas de tokens representan un punto intermedio entre una oferta inicial de acciones (*Initial Public Offering*, en inglés) y una campaña de crowdfunding [641]. Quienes invierten en tokens o *appcoins*, lo hacen por tener una expectativa tanto (i) en que la propuesta de valor fondeada tendrá tracción y venderá muchos tokens, (ii) como en el *roadmap* diseñado por los emprendedores y normalmente publicado en un *White Paper* [642] on line, que, a diferencia de un prospecto de emisión convencional [643], no se encuentra regulado en su contenido. Si la expectativa del adquirente de tokens se cumple, el valor de las *appcoins* subirá, con lo cual su reventa será rentable; o, en el caso de que el token confiera un derecho de acceso o de uso a determinados servicios digitales, los tokens *holders* pagarán un menor precio por acceso o uso por haber invertido en la etapa de *pre-seed capital*.

Más allá del caso *TheDAO* ya analizado, en el período comprendido entre 2016 y 2019 hubo 1392 proyectos fondeados mediante ICOs en 56 países, el 90% de los cuales se lanzó en la plataforma de Ethereum [644]. Sólo en 2019, se captaron 14.800 millones de Dólares en ICOs [645]; en 2018 se alcanzó el máximo de 24.200 millones de Dólares de fondeo vía ICOs [646] –teniendo en cuenta el valor antes del cryptomarket crash o *CryptoWinter* [647]–; y en 2017 se captaron 6.230 millones de Dólares vía ICO [648]. En el período 2016-2019, casi el 98% de los proyectos emitió *utility tokens*, y la mayoría de las empresas

fondeadas fueron startups formadas por entre 3 y 12 participantes [\[649\]](#).

Estos volúmenes de inversión y fondeo han llamado la atención de la OECD, que ha afirmado en un informe de 2019 que las ICOs permiten una forma innovadora e inclusiva de financiar a las PyMES y que, además, permiten potencialmente la creación de valor a través los efectos de red y por ganancias de eficiencia por el uso de *blockchain*, lo que puede producir ahorro de costos y tiempos [\[650\]](#).

Ahora bien, si bien se trata de una novedosa forma de fondear emprendimientos, no está exenta de riesgo, sea en forma de estafas (muy abundantes), sea en forma de ataques cibernéticos, y, además, está sujeta a los riesgos del negocio fondeado *per se* [\[651\]](#).

3.2.3.2. Generación eléctrica distribuida

Otro ejemplo del escenario en que la *blockchain* alivia fricciones transaccionales es en el ámbito de la generación eléctrica (solar) distribuida. En estos casos, la *blockchain* permite que se estructuren mercados peer-to-peer donde los generadores domiciliarios pueden vender (y comprar) el excedente de energía que producen con paneles solares domiciliarios. La energía renovable puede ser tokenizada, y tranzada en una *blockchain* utilizando una appcoin nativa, utilizando *Smart Contracts* para gestionar los excedentes de energía, gestionando su venta y su cobro de manera automática, y recurriendo a la infraestructura de transporte de energía ya establecida [\[652\]](#).

3.2.4. Good Blockchain Governance

Vistos entonces los tres posibles contextos principales de interacción entre la *blockchain* y el Estado de Derecho, la primera pregunta que asoma es si conviene o no conviene que el Estado fije (o intente fijar) criterios generales, estándares, sean *soft law* [\[653\]](#) o *hard law*, que estipulen reglas mínimas de gobierno intra-*blockchain*, al menos en relación a las *blockchains* públicas. La

segunda pregunta es si acaso el Estado tiene la posibilidad y capacidad técnica de influir de tal modo en las arquitecturas de un sistema descentralizado que está en todos lados y en ninguno, a la vez.

Yeung afirma que en el futuro emergerán principios y normas de buen gobierno en *blockchain*, aunque quizás no tengan la forma de una ley, sino de lineamientos o directrices ^[654].

3.3. *Tokens vs. Law: perspectivas en el derecho comparado*

En este apartado se pasará revista al novedoso fenómeno de la representación digital de activos. A tal fin, se desarrollará el concepto de token digital, se analizarán sus diversas especies, se describirá el proceso de tokenización y se analizarán casos de uso relevantes. Cuando sea conveniente o necesario, se analizarán las posturas regulatorias más relevantes en relación a la denominada *taxonomía* del token.

3.3.1. *Taxonomía del Token* ^[655]

El hecho económico precede siempre a la regulación. Esto es tan obvio como el dato sociológico que los nuevos negocios –la sustancia– normalmente no pueden aguardar tipificaciones legales –la forma–, y se gestan en la tangente que se forma entre la tipicidad social, la autonomía de la voluntad, y la creación de valor sustentable.

Esta situación genera un natural retraso en el diseño regulatorio, y una expectativa legítima en el emprendedor de que la regulación ulterior será eficiente y respetuosa de las garantías constitucionales de emprender, innovar, crear y disponer de la propiedad privada.

Sin embargo, cuando el hecho económico se apalanca en la tecnología, la demora regulatoria se agrava ya que los reguladores, además de conocer sobre la materia propia de su *expertise*, *deben incorporar conocimientos técnicos que no son tan fácilmente asequibles*. Para peor, muchas veces, no existen canales de diálogo efectivos y asertivos entre reguladores y tecnólogos, y la regulación

–temprana, tardía y/o inadecuada– no sólo puede afectar garantías constitucionales del emprendedor o del innovador, sino también frenar o prohibir la innovación. Y no parece sensato frenar ni prohibir la innovación cuando los signos de los tiempos muestran el surgimiento firme de una *Cuarta Revolución Industrial*.

Las tecnologías DLT, específicamente la *blockchain*, han abierto nuevas posibilidades para financiar emprendimientos de base tecnológica *early stage* o el lanzamiento de nuevos productos o servicios digitales, “*tecno-democratizando*” el acceso al financiamiento y el lanzamiento global de bienes y servicios digitales, pivotando sobre variopintas aplicaciones de la cadena de bloques, dando lugar a una nueva disciplina dada en llamar *Token Economics* [\[656\]](#), que está impactando de lleno en la regulación de una ya muy establecida disciplina, el *Corporate Finance* [\[657\]](#), desarrollada a partir de la *Securities Act* de 1933 y la *Securities Exchange Act* de 1934 de EE.UU, leyes éstas que fueron la respuesta regulatoria a abusos bursátiles que motivaron el Crack de 1929, una crisis de profundo impacto que demuestra, con sabor amargo, que el hecho económico siempre precede a la regulación.

Y cada vez que pueda, el fenómeno económico tratará de posicionarse en un lugar a donde no llegue el ojo regulatorio.

Ahora bien, el ámbito bursátil es fuente inagotable de innovación, autonomía de la voluntad, y también de abusos y sofisticados delitos de cuello blanco [\[658\]](#). Es, también, un mercado “de capitales” con altas y costosas barreras de ingreso tanto para empresas establecidas como para nuevos emprendimientos, cuya simplificación creciente, al menos en lo atinente a la ON PYME, es quizás el mayor mérito de nuestra Comisión Nacional de Valores (CNV).

Sin embargo, se percibe en los reguladores bursátiles a nivel global cierta actitud reticente a fomentar la tecno-democratización del acceso al financiamiento para lanzar nuevos productos y servicios digitales y globales, apreciándose una larga lista de advertencias al público inversor [\[659\]](#) y variopintas regulaciones que abordan la disciplina del *Token Economics*,

justificadas –en muchos casos, con razón– en una protección del inversor, extrapolando criterios tutelares del Siglo XX que nunca pudieron si quiera concebir la utilidad, aplicación, seguridad, trazabilidad, y demás virtudes de los Tokens del Siglo XXI.

Se trata de tensiones que demuestran, a todas luces, el potente choque de fuerzas subyacentes entre tecnologías que proponen democratizar el acceso al financiamiento en un mercado global, versus reguladores locales que pretenden mantener el monopolio del acceso al financiamiento en su jurisdicción, o en otros términos, la altura de la barrera de acceso al mercado de capitales en beneficio de los incumbentes. Regulaciones inadecuadas que pueden llevar consigo el riesgo de frenar o directamente prohibir formas innovadoras de financiar emprendimientos o el lanzamiento de productos o servicios digitales.

3.3.1.1. Primeros acercamientos regulatorios y legislativos. Token Taxonomy Act de 2019.

En Argentina, la CNV con fecha 4/12/2017 rápidamente se posicionó emitiendo una *alerta* al público inversor sobre emisión de tokens [\[660\]](#). Pocos días después, el Congreso sancionó la Ley N° 27.430, gravando en el Impuesto a las Ganancias, con un alícuota del 15%, todas las ganancias obtenidas por enajenación de monedas virtuales [\[661\]](#).

CNV definió a la *blockchain* como un “*inventario de existencia electrónico no modificable*” de todo el sistema de transacciones que es mantenido por varios partícipes en una red de computadoras, que almacena de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión. Es decir, que la cadena de bloques o *Blockchain* actúa como un libro abierto donde se registran todas y cada una de las transacciones efectuadas”. La CNV se refirió también a la tokenización afirmando que comprende desde la emisión de monedas virtuales, hasta un token digital que puede representar una acción en una empresa, un bono prepago para servicios futuros o, en algunos casos, no ofrecer ningún valor discernible.

44 días después de la alerta de la CNV, la International Organization of

Securities Commissions (IOSCO) ^[662] publicó un comunicado de prensa alertando sobre preocupaciones generadas por emisión de criptomonedas a nivel global. El comunicado evidencia una clara preocupación por estas nuevas formas de acceso al financiamiento, denuncia la existencia de posibles fraudes, y resalta que la comercialización online de tokens los sustrae de las jurisdicciones en que residen los inversores que los adquieren o los emisores que los emiten.

64 días después de la alerta de CNV, en un comunicado conjunto emitido por la Comisión Nacional del Mercado de Valores (CNMV) y el Banco de España (BCE) ^[663], los reguladores españoles, quizás con mayor precisión que nuestra CNV, distinguen entre la emisión propiamente dicha de criptomonedas (Initial Coin Offerings –ICOs–) y la emisión de “derechos de diversa naturaleza” denominados *tokens* o vales.

A su vez, los reguladores españoles ya introducen una clasificación esencial de los tokens en (1) *security tokens*, que reconocen un derecho a participar en futuros ingresos o en la plusvalía de la entidad emisora, y (2) *utility tokens*, que se limitan a dar acceso a un servicio, o conferir el derecho a recibir un producto, con la posibilidad o no de negociar estos tokens en mercados secundarios.

A nivel comunitario, Suiza ha sido pionera y es referente mundial en la regulación legal de la tokenización, impulsada quizás por la participación de UBS en la Fundación Ethereum. Suiza reconoció rápidamente diferentes tipos de Tokens (asset, utility y payment tokens) ^[664] e impulsa el estudio profundo del Token Economics para optimizar su regulación sin afectar la innovación ^[665].

El enfoque suizo considera que el *payment token* es sinónimo de criptomoneda y su única funcionalidad es servir para transaccionar pagos. El *utility token* permite acceder a productos o servicios digitales. El *asset token* representa un activo, que puede ser físico (off-chain), participaciones en sociedades, o en flujos de fondos generados por emprendimientos, instrumentos de renta fija, o en general, situaciones jurídicamente análogas a

las que representa emitir acciones u obligaciones negociables, o participar en contratos derivados.

Del otro lado del Atlántico, resulta muy interesante analizar algunos pasos regulatorios en Estados Unidos, un mercado en el que también se registran movimientos tectónicos motivados por la nueva disciplina del Token Economics.

En Diciembre de 2017, el Presidente de la SEC^[666] sostuvo que la SEC intenta establecer una regulación específica en la materia que, a la vez, impulse la innovación responsable y proteja a los inversores y a los mercados.

En este sentido, doctrina especializada ha sostenido^[667] que la SEC ha ido modificando, a lo largo del tiempo, su entendimiento sobre cuándo un Token debe ser considerado un Security conforme a la legislación y jurisprudencia aplicables^[668], y de a poco ha ido ganando protagonismo la figura del *Utility* token, como algo distinto –tanto en su naturaleza económica como jurídica– al Security token. En palabras del Presidente de la SEC, un Token no será un Security regulado si sus adquirentes no esperan razonablemente que una persona o grupo gestor preste servicios de gestión empresarial.

También es interesante traer a colación que con fecha 9/04/19 se presentó al Congreso de Estados Unidos un proyecto de ley que aborda directa y muy pragmáticamente la *Taxonomía* de los Tokens^[669], y que los define^[670] y propone (i) excluir los Tokens digitales de la regulación de Securities de los años 1933 y 1933; (ii) instruye a la SEC a modificar su regulación respecto a unidades digitales protegidas con encriptado de llave pública^[671]; (iii) propone modificar el tratamiento tributario de monedas digitales tenidas en cuentas de retiro; (iv) crea una exención fiscal por intercambios de monedas digitales; y (v) establece un mínimo no imponible respecto de ganancias obtenidas por venta de monedas digitales.

3.3.1.2. *Security Token Offering (STO)*

Hablar de STOs es hablar de una emisión de un token que cumple (o debe

cumplir) las normas bursátiles aplicables a los títulos valores con oferta pública, las que son generalmente muy similares a las que se exigen para una IPO.

Evidentemente, estos resguardos ofrecen un marco de seguridad al inversor –que generalmente debe ser un inversor calificado, i.e. con ingresos no menores a U\$D 200.000 por cada uno de los dos años previos a la inversión de que se trate– varias veces superior al que ofrece la emisión de *Utility* token no regulado. Lógicamente, el proceso de verificación de los requisitos de un STO es más caro que un ICO y no tan rápido, pero es más barato que una IPO que permite acceder a mercados globales como el NASDAQ o el NYSE.

Se ha señalado que un STO puede estar o no vinculado al capital social de la compañía que los emite, y que normalmente confieren derechos de voto, derecho a percibir dividendos periódicos, y otras cláusulas, que pueden ser programadas y ejecutadas vía *Smart Contracts* [\[672\]](#).

En el caso de EE.UU, un STO debe ser previamente registrado en la SEC, bajo estas posibles formas: Reg S, Reg D, Reg A+ y Reg CF (crowdfunding) [\[673\]](#). La Reg S aplica a STOs de empresas extranjeras, que cumplen en su país de origen las normas aplicables a los títulos valores con oferta pública. Permite que un token pueda ser adquirido por un inversor de EE.UU. La Reg D, por su parte, permite que un token sea adquirido por un inversor calificado, pero el monto total de la emisión no puede superar los 5 millones de Dólares y el token no puede ser comercializado durante los dos años siguientes a su compra; mientras que la Reg A+ tiene un límite de emisión de hasta 50 millones de Dólares, pero exige dos años de información contable, económica y financiera del emisor, con lo cual muchas startups quedan fuera de juego. Finalmente, Reg CF permite captar hasta 1.7 millones de Dólares, pero el comprador del token debe retenerlo por 12 meses obligatoriamente [\[674\]](#).

Se ha señalado que la mayoría de STOs se emiten en Ethereum, con el protocolo ERC20 siendo el más usado, y está en camino el nuevo estándar diseñado específicamente para STOs: ERC 1400 [\[675\]](#). También se ha resaltado que la gran mayoría de los STOs –99%– terminan en casos de éxito,

a diferencia de los ICOs donde la tasa de éxito no llega al 10% ^[676].

La programabilidad de un STO permite que desde su diseño, se prevean funcionalidades tan relevantes como:

“... issuers need to be able “force” certain functionality on token holders (appropriately disclosed) including **forced upgrade, transfer, burn and mint**. Burning means destroying the tokens, and minting means creating tokens, in each case in a cryptographically secure manner. Forced transfer, burning and minting need to be available in the event of a court order, but also offer necessary functionality if tokens are lost or stolen. Upgradeability is important because the state-of-the-art for security tokens continues to evolve at a rapid pace.” ^[677] (el resaltado es mío).

3.3.1.2.1. *Simple Agreement for Future Token (SAFT)*

En el ámbito de los STOs, debe traerse a colación la utilización de los SAFTs ^[678]. Es un contrato que es *per se* un contrato de inversión, i.e., un tipo de *security* para la SEC, que se suscribe entre (i) los desarrolladores/emprendedores que lideran el proyecto a fundarse vía un futuro STO o ICOs, según el caso ^[679], y (ii) ciertos inversores calificados que pueden adquirir los tokens a emitirse. El nombre recuerda a los SAFEs de Y-Combinator ^[680], muy utilizados para *early stage seed capital financing*, en el mundo *off-chain* donde se emiten participaciones sociales “estándar”, y en el cual el SAFT está inspirado. Es perfectamente posible que se celebren ambos instrumentos por separado entre los mismos inversores y los mismos emprendedores.

Los SAFTs son un tipo de *Smart Contract*, a los que se les asigna una dirección en el plataforma *blockchain* en la cual, en el futuro, se crearán los tokens que corresponden a la dirección del SAFT. Permite que el inversor

reciba los tokens en un momento futuro, pero con un importante descuento en el precio [\[681\]](#). El SAFT *per se* debe registrarse en la SEC, pero no es necesario cumplir mayores formalidades en esta instancia inicial, ya que no hay aún creación de tokens. Es decir, el inversor tiene como resguardo el SAFT, pero no tiene aún el token [\[682\]](#). Una vez que el desarrollo está terminado, se crean los tokens que deberán inscribirse en la SEC en alguna de las categorías aplicables ya vistas más arriba, de modo de garantizar que se cumplan las normas de KYC y AML, pero se entregan a un precio preferencial a los inversores que hayan celebrado SAFTs.

No obstante su utilidad, se ha sostenido que a pesar de haber sido muy utilizados para las colocaciones más grandes de tokens, el reciente criterio expansivo de la SEC ha puesto la mira en los SAFTs, desdibujando la línea divisoria entre STOs y las ICOs que seguidamente se analizan, lo que afecta la utilidad de esta figura [\[683\]](#). Esto ha motivado que reputados doctrinarios alerten al público en general sobre los riesgos inherentes al uso de SAFTs [\[684\]](#). Al momento de escribirse este Manual, la discusión sobre la utilidad o no de los SAFTs, y la naturaleza jurídica de los tokens que son su objeto, sigue abierta.

3.3.1.3. *Initial Coin Offerings: Soft Cap y Hard Cap*

Cambiando de perspectiva, cuando se habla de ICOs, ya nos alejamos de los ámbitos de regulación bursátil de los STOs, y nos adentramos ahora en un área más opaca, donde –aparentemente– han existido más casos de estafa que de éxito [\[685\]](#).

Alina Myalo puntualiza los siguientes caracteres –i.e. cláusulas– usuales y esenciales en la estructuración de una ICO [\[686\]](#):

“Before launching an ICO, the development team determines the tasks for which it is necessary and indicates 2 digits in its White Paper: the minimum and maximum, called the Soft Cap

and the Hard Cap. **The Hard Cap defines the final goal, the upper limit of the amount of money invested, the most desired result.** This is a very important indicator, precisely, because many cryptocurrencies have a limit on the total number of units in circulation. This, in turn, is one of the most important factors influencing the value of the coin, in addition to supply and demand. **The Soft Cap is the minimum required amount of investment for the team to proceed the project** implementation according the plan. **If it is not reached within the specified period, the contract is closed, and it automatically returns all funds raised to the depositors. If the Hard Cap is reached, the sale of tokens stops.** However, after overcoming the Soft Cap, investors control only the purchased tokens and cannot control the money invested or withdraw part of the investment. In case of the ICO, **developers return funds to investors only if they failed to collect the required amount during the Soft Cap.** If the required amount of the Soft Cap is reached, investment cannot be refunded to token holders even if the project is stopped or it is terminated along the way. After the Soft Cap, fundraising continues until the Hard Cap. **Sometimes the amount exceeds the set maximum value and continues to increase.** In this case, the organizers must terminate the ICO and return the extra funds to investors. Unfortunately, the organizers do not always meet these obligations.”^[687] (el resaltado es mío).

3.3.1.4. Tokens: substance over form, STOs vs. ICOs.

Visto lo anterior, se puede adelantar ya una definición de tokens como una representación digital de valor emitida por una entidad privada que funciona como medio de intercambio, unidad de medida o reserva de valor. Token y moneda virtual (*virtual currency*) son conceptos sinónimos. Bitcoin es el (primer) token por excelencia. Se resalta nuevamente la esencial diferencia entre (i) *Security* tokens, los tokens cuya *naturaleza jurídica* encaja en la

definición de acciones, participaciones, bonos y en algunos casos, derivados; y (ii) *Utility* tokens, tokens que operan como un vale o ficha, que permite el acceso digital a servicios o aplicaciones, en definitiva, funcionan como mecanismos de intercambio y de pago.

Como se ha analizado, los *Security* Tokens son asimilados a títulos valores, tanto en Argentina como en España, aunque la CNMV ha sido más flexible al reconocer de modo muy expreso la diferenciación esencial entre *Utility* y *Security* Tokens.

La emisión de *Security* Tokens se denomina *Security* Token Offering (STO), mientras que la emisión de un *Utility* Tokens se denomina *Initial* Coin Offering (ICO). Evidentemente un STO cae dentro de los poderes regulatorios de los supervisores bursátiles en todo el mundo; pero no está claro que las ICOs deban quedar comprendidas en tales regulaciones, y esto puede haber llevado a muchas empresas a “disfrazar” como ICOs lo que en realidad es un STO. En estos casos patológicos, es evidente que los reguladores tienen competencia para actuar puesto que la naturaleza económica de la transacción subyacente (STO) sella la suerte jurídica del instrumento utilizado (título valor regulado “por accesión”). *Contrario sensu*, una emisión genuina de ICOs, esto es, *Utility* Tokens, no debería caer dentro del poder regulatorio de los supervisores bursátiles, y tal es el espíritu – correcto a mi entender– que refleja la *Token Taxonomy* Act recientemente presentada al Congreso de Estados Unidos, y también es el entendimiento que subyace en los SAFTs.

En España, con fecha 20/09/18 la CNMV emitió un documento titulado “Criterios en relación a ICOs”^[688], donde puede advertirse que el regulador modifica su criterio regulatorio expuesto en el comunicado conjunto emitido junto con el BCE en Febrero de 2018, para directamente excluir de su competencia a los Tokens que en los que no quepa razonablemente establecer una correlación entre (i) las expectativas de revalorización o rentabilidad del Token y (ii) la evolución del negocio subyacente. El viraje es trascendente, y va en la dirección correcta.

Como conclusión preliminar, pareciera que el vaivén regulatorio y legislativo de EE.UU y España sobre la *Tokenización* da cuenta que las regulaciones bursátiles del Siglo XX no son adecuadas para regular los

fenómenos tecnológicamente complejos y económicamente novedosos del Siglo XXI. Se requieren herramientas nuevas para gestionar realidades nuevas y mientras se logra descifrar cuáles son éstas nuevas herramientas, podemos simplemente dedicarnos a experimentar, a jugar como niños en un arenero, creativamente, y ver qué pasa. Este enfoque es práctico, adecuado, pro-innovación, pro-consumidor. Esta es la esencia del modelo *SandBox* ^[689] inglés, que se analizará más abajo en 3.4.1.1.1., pionero en articular puntos de contacto entre la innovación y el mercado en un ámbito de libertad y mínima regulación preventiva, y el cual planea seguir España en el corto plazo con su Anteproyecto de Ley para la Transformación Digital del Sistema Financiero ^[690].

3.3.1.5. Cuando la claridad regulatoria es necesaria

Las álgidas discusiones doctrinarias sobre el SAFT y las distintas percepciones legales sobre las STOs y ICOs en uno de los mayores mercados del mundo, como lo es EE.UU., no es una buena noticia para el desarrollo de la criptoconomía, la *blockchain* y los contratos inteligentes. El fenómeno se replica en muchas jurisdicciones.

En este sentido, y en lo que a EE.UU. respecta, los profesores Wright y Rohr ^[691] han afirmado que tanto los Legisladores como los Tribunales deben reconocer las distintas características intrínsecas y extrínsecas de los Security y los Utility tokens.

Así, en opinión que se comparte, proponen que ciertos tipos de *Utility* tokens queden exentos de las obligaciones de inscripción y registro en la SEC conforme al Art. 5 de la Ley de Títulos Valores de 1933; la SEC como ya se señaló más arriba al analizar el caso *TheDAO*, tiene una posición fijada sobre qué entiende por Security token aplicando el precedente *Howey* ^[692]. Sostienen los autores citados que las normas vigentes de registración para títulos valores convencionales no funcionan ni se adaptan bien para ciertos tipos de tokens digitales, y no tienen en cuenta las particularidades de la tecnología subyacente ^[693]. Por la claridad conceptual y la importancia del

tema abordado, nos detendremos para analizar en profundidad la propuesta de Wright y Rorh.

3.3.5.1.1. Precisiones terminológicas

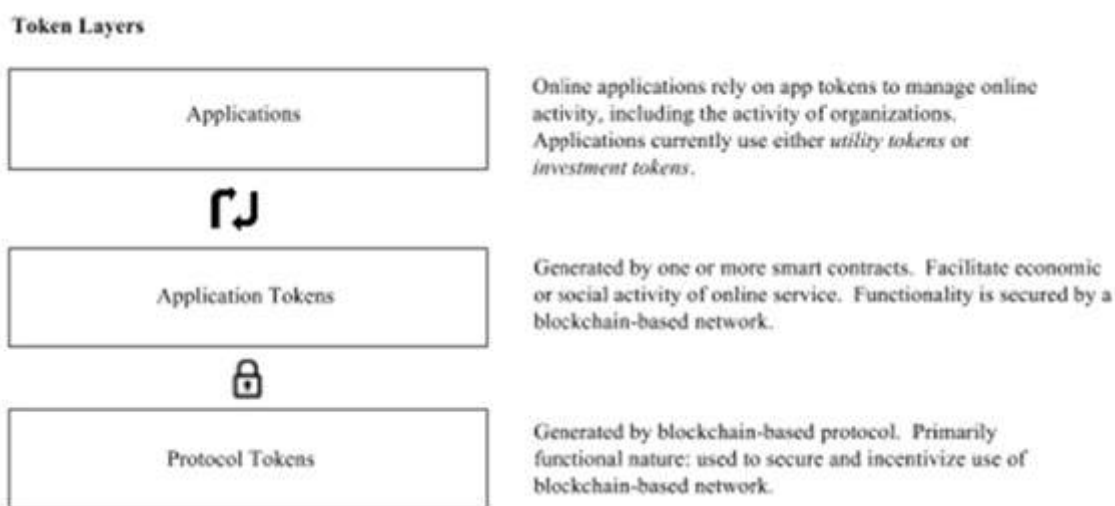
Señalan Wright y Rohr que deben distinguirse los Tokens de Protocolo, por un lado, y los App Tokens, por el otro [\[694\]](#). Los primeros son utilizados por las *blockchains* públicas para retribuir trabajos de mantenimiento y minado que consumen muchos recursos debido al protocolo de PoW empleado, son una *recompensa*, y en el caso de Bitcoin, el *black reward* es la única forma de emitir nuevas bitcoins al mercado. En el caso de Ether, también un token de *protocolo*, se puede comprar y se utiliza para pagar el servicio brindado por la EVM para procesar contratos inteligentes. En alguna medida, el Ether es una unidad de cuenta que permite pre-pagar el acceso a una computadora virtual descentralizada, mantenida por los miembros de la red Ethereum [\[695\]](#).

Los App Tokens, en cambio, son un fenómeno bien distinto. Son creados mediante *Smart Contracts* de Ethereum, normalmente, y permiten asignarles derecho de voto, de participación, de uso o consumo de bienes o servicios digitales. Se crean normalmente con un contrato inteligente estándar, llamado ERC20, que permite crear un token con menos de 100 líneas de código [\[696\]](#). Quien adquiere un App token tiene control total sobre el mismo, y a su turno el *Smart Contract* lleva un registro de quién tiene el token en cualquier momento dado. El creador del token puede reconocer derechos, privilegios y recompensas dentro de una aplicación o en relación a un servicio digital.

Dentro de los App Tokens, se llaman *utility tokens* a los *app tokens* que se limitan a otorgar un derecho de uso, o de acceso, a un servicio o plataforma digital que brinda determinados servicios digitales. Los utility tokens pueden también otorgar derechos de voto, normalmente en relación a modificaciones o evoluciones del servicio digital cuyo uso o acceso permiten [\[697\]](#). Citan como ejemplos de utility tokens al Status Network Token [\[698\]](#) y al Basic Attention Token [\[699\]](#). Otra especie de App Token, son los *investment tokens*:

confieren un derecho de uso o acceso, y además, el derecho a participar en las ganancias del proyecto financiado [700]. El DAO Token es un ejemplo de esta especie. Otro ejemplo de este tipo de token de inversión es BCAP Token [701]. El cuadro abajo, tomado de Wright y Rohr, escenifica los tres niveles de Tokens:

Imagen 12
(Wright y Rohr, p. 26)



3.3.5.1.2. Proceso de venta de App Tokens

Wright y Rohr describen [702] el proceso de comercialización de App Tokens, indicando que todo inicia con un White Paper, donde se describe el proyecto en sí, la hoja de ruta del desarrollo, los tipos de tokens que se crearán, el equipo de desarrollo, sus asesores y la distribución propuesta para los tokens, incluyendo los que corresponderán a los desarrolladores.

Luego de hacer público el White Paper, se pone a disposición de todo el mundo en formato *open source* el código de programación del proyecto, el que suele ser auditado para detectar *bugs*, incluso ofreciendo recompensas para quien detecte algún error de programación [703].

El inicio de ventas de los tokens se difunde anticipadamente en canales online muy específicos (Reddit, Slack, etc), y su apertura funciona como un evento de crowdfunding mundial. Los inversores que los adquieren los reciben directamente en su *Wallet*. Muchas ventas tienen un límite, el *Hard Cap*, y el proceso de venta demora segundos o sólo minutos en muchos casos [\[704\]](#). Una vez vendidos, los tokens normalmente no pueden ser devueltos contra reembolso al emisor, y su transferibilidad es libre [\[705\]](#) a través de plataformas de venta –*Exchanges*– en todo el mundo, que le dan mercado secundario si aceptan listarlos [\[706\]](#). En éstas plataformas, pueden re-venderse tanto los utility tokens como los investment tokens, por igual, y existen muchos casos en los que el valor del token se apreció exponencialmente [\[707\]](#).

Los fondos recaudados por la venta de tokens van a la organización que vende los tokens, la que puede asumir distintas estructuras jurídicas: sociedades comerciales, fundaciones, o incluso sin forma jurídica alguna, como lo fue el caso *TheDAO*. Un formato jurídico usual es el de fundación constituida en una jurisdicción *crypto-friendly*, como el cantón suizo de Zug. A enero de 2018, el monto total de 540 app tokens comercializados alcanzó los 365.000 millones Dólares [\[708\]](#), y en muchos casos, la venta fue colocada en su mayoría en un número pequeño de compradores [\[709\]](#).

Dada la existencia de casos de tokens que se apreciaron exponencialmente, muchos utility tokens demostraron tener también un *valor especulativo*, quizás apalancado por el hecho que el número de tokens emitidos es fijo y limitado [\[710\]](#) y por los efectos de red asociados. Con razón, sostienen Wright y Rohr que *blockchain* le está haciendo a las finanzas lo mismo que Internet le hizo al copyright en los noventa [\[711\]](#). Dicen los autores –en opinión que se comparte:

“In effect, the distributive power of the Internet is being combined with the raw power of a blockchain to manage and transfer assets globally. **This combination has extraordinary**

potential for capital formation, streamlining a once cumbersome process of raising funding and holding out the hope of democratizing access to capital and unleashing untapped entrepreneurship. At the same time, however, when **digital goods**—which are meant to be consumptive in nature—are **tokenized and are sold online using blockchain technology, they begin to resemble securities.** Just like how blockchains break down barriers related to the sale of digitized securities, blockchains also decrease the cost of selling and managing the sale of digital goods, making them highly liquid. These goods become capable of being traded or transferred by anyone and to anyone around the globe, all facilitated by token exchanges.”^[712] (el resaltado es mío).

3.3.5.1.3. *El régimen federal de títulos valores regulados en EE.UU.*

Señalan Wright y Rohr que los *investment* tokens caen dentro del *Howey test* sin mucho que analizar^[713], pero no hay tanta claridad respecto de los *utility* tokens, que combinan un uso funcional, de uso o consumo, y, además, pueden tener valor especulativo si se aprecian, y su reventa es muy fácil en plataformas de mercado secundario de app tokens, *Exchanges*.

Esta naturaleza dual de ciertos utility tokens complica su encuadramiento bajo la legislación federal en EE.UU.^[714], ya que en algunos casos predominará de manera clara el factor funcional –i.e, consumo/uso–, pero en otros será difícil trazar la divisoria de aguas^[715]. En este sentido, señalan los prestigiosos doctrinarios en relación a los utility tokens:

“These tokens, by definition, **entitle their holders to some element of use or consumption, but the active secondary market for tokens also allows them to be viewed as an investment opportunity.** Because these tokens entitle the holder to use, consume, or access an online service or serve other functional purposes (for example, participating on a

messaging platform or surfing the Internet without ads), elements of a consumption purpose are present. Naturally industry participants have focused on this consumptive aspect of app tokens to argue that as a class, they fall outside of the securities laws.”^[716] (el resaltado es mío)

Muchos tokens son *híbridos*, y mezclan y confunden elementos funcionales y de inversión. Señalan los autores citados que la publicidad que se haga es importante, así como el tiempo que transcurre entre que se comercializan y la aplicación está en funcionamiento^[717]. Por todo esto, se afirma, con razón, que:

“Given the factually intensive nature of this inquiry, no categorical answer is possible. **The security status of utility tokens will depend on a mix of facts and circumstances that will differ for each token.** Certainly, sellers of utility tokens can avoid taking certain actions that make their token sale resemble an offering of securities—for example, by advertising it as an investment opportunity or targeting the sale of tokens to investors, venture capitalists, or hedge funds. But, the novel way that tokens combine both speculative and consumptive value alongside the undeniable fact that some token purchasers will be motivated by an expectation of profits no matter how the token offering is conducted preclude any easy or definite answers at this stage.^[718]” (el resaltado es mío)

En la legislación federal de EE.UU, existen ciertas excepciones que permiten no tener que previamente registrar un *security* en la SEC^[719], pero señalan los autores que no han sido pensadas para el nuevo fenómeno de la tokenización, ni tienen en cuenta los atributos esenciales de la *blockchain*. Mayores precisiones son requeridas, a nivel de *lege ferenda*^[720].

3.3.5.1.4. Factores intrínsecos y extrínsecos

Siempre siguiendo a Wright y Rorh, señalan los autores que hay países que han fijado una posición clara y contundente (y favorable) respecto a que los *utility* tokens no son títulos valores regulados, ejemplificando con Singapur ^[721]. Estas certidumbres atraen inversión, que busca jurisdicciones amigables a la innovación ^[722], mientras que una actitud opuesta, producirá, en EE.UU y también en Argentina, una migración de talento e innovación hacia tierras más amigables:

“Sales of app tokens and the online projects that they support, on the other hand, can be taken outside the purview of U.S. law and regulators more cheaply and much more easily. **A haphazard or over-inclusive regulatory approach will drive token sales outside of the U.S. and out of the reach of U.S. purchasers.** The relevant question for regulators, then, is whether maintaining a particular regulatory approach is worth driving these projects outside of the U.S., **depriving would-be U.S. end users of the ability to use new digital technology, and ultimately forcing U.S. companies to forego the new generation of financial techniques.** Significantly, because utility tokens are the key to using the services that they fund, a regulatory approach that drives token sales away from the U.S. is ultimately keeping those services out of the reach of all U.S. citizens, even those who have only an expectation of consumption.” ^[723] (el resaltado es mío)

Por ello, los autores proponen que la autoridad bursátil –nuestra CNV– ^[724]: (i) emita lineamientos claros y precisos sobre qué factores evalúan para definir la naturaleza jurídica de un token como security o utility; (ii) estos lineamientos deben atender a los factores intrínsecos del token que preponderan: uso/consumo ^[725] vs. inversión; (iii) estos lineamientos

debieran también atender a los factores extrínsecos ^[726] que rodean la venta del token, especialmente los relacionados a los tokens que se asignen a los desarrolladores ^[727]; y (iv) cree una nueva excepción, específica, para no registrar security tokens que cumplan condiciones determinadas *ad hoc* para este nuevo tipo de producto de inversión, ya que las actuales no encajan bien con el sustrato tecnológico de la *blockchain*, y a veces exigen condiciones ilógicas para las DLTs, como tener que contratar un agente de registro –algo que puede ser hecho con un *Smart Contract*, sin tener que contratar a un intermediario que solo agrega costos ^[728].

Finalmente, Wright y Rorh también proponen ciertos cambios legislativos, en un formato de *safe harbour*, donde se proteja a los *Exchanges* donde estos tokens pueden ser vendidos y a veces también revendidos. Esto es importante especialmente para la responsabilidad civil eventual que puede surgir en cabeza de los *Exchanges*, si se determinase –*ex post facto*– que ciertos tokens son considerados investment tokens por parte de la SEC. Pero el *safe harbour* es también necesario, principalmente, para no frenar la compra y la venta de genuinos utility tokens ^[729].

3.3.1.6. DAICOs y IEOs

Pero la cuestión no se termina en STOs y ICOs y su encuadramiento legal. La tecnología avanza más rápidamente que la doctrina. Ni hablar que las leyes y regulaciones.

A esta primera bifurcación analítica entre utility y security tokens, ya se puede agregar otra, de muy reciente creación, que es propia de las DAOs, y se denomina DAICOs. Una DAICO significa *Decentralized Autonomous Initial Coin Offering* ^[730], y como su nombre indica, es una ICO emitida por una DAO.

Una DAICO está basada en un contrato inteligente, que regula todas las acciones desde la atracción y captación de fondos, hasta su utilización con fines determinados: serán los *finis constitutivos* de la DAO de que se trate.

Una vez que el proceso de venta finaliza, los DAICOs quedan gobernados

por el *Smart Contract*, que puede bloquear los fondos recaudados para que no sean de libre disponibilidad hasta que determinados períodos o hitos se cumplan –similar a un *vesting* agreement de acciones–, lo que también garantiza que el equipo gestor del emprendimiento no abuse de su poder y no manipule los precios del token. Asimismo, libera los fondos al equipo gestor de acuerdo a un cronograma de trabajo determinado, que garantiza al inversor el destino real y la aplicación final de los fondos para los fines comunicados [\[731\]](#).

Alina Myalo puntualiza los siguientes caracteres de una DAICO:

“The difference between the DAICO and the ICO begins after the first stage when a mechanism called “tap” is launched. **Tap allows tokens holders to control how much money is available for the team.** The tap determines the amount per second that the development team can withdraw from the contract. Such a tool gives token holders control over the spending of raised funds and guarantees the security of their own investments. **Payments to developers are not made once, but gradually, for example, once a month.** If they need more than it is written in the Smart Contract, then this question is put to the vote. Token holders can either approve this proposal or not. So, the DAICO’s key advantage over the ICO is that **holders have a greater control with a possibility to vote and restrict access to investments**, which negates the risk of manipulation of tokens and funds by the team (...) implementation of the DAICO platform **increases the accountability of developers to investors** and gives the latter additional **guarantees that extra investments will be returned at the initial stage.** In general, the DAICO solves the problem of irrevocable overspending of ICOs. In addition, if the token holders are dissatisfied with the development of the project, they can vote for the refund of the funds left on the Smart Contract at any stage of product development.” [\[732\]](#) (el

resaltado es mío).

Finalmente, en 2018 también aparecieron las IEOs, *Initial Exchange Offerings*. Nuevamente siguiendo a Myalo y tomando prestada su abrumadora claridad, en relación a las IEO señala:

“This is a new way to attract investment for various companies, where the **cryptocurrency exchange is directly involved in the selection of projects, organization and sale of tokens**. In fact, the IEO is a new ICO, where the exchange becomes the key marketing partner of the project, and the listing of coins is carried out only a couple of days after the campaign ends. Actually, the cryptocurrency exchange distributes digital assets among interested investors, who are verified users of the trading platform. There are several advantages of the IEO over the disadvantages of the ICO: (1) The **risk of scams for investors is lower**. The project is launched at the exchange after profound verification. The exchange rejects a dubious project to keep up its reputation. (2) Listing of new tokens is faster. (3) Redistribution of costs becomes available: according to Autonomous Research, listing an ICO token on a cryptocurrency exchange can cost promoters anywhere between \$ 1 million and \$ 3 million. An IEO project has lower costs for listing. (4) The financing rate is higher: in the ICO, the primary distribution of tokens may last for several days whereas in the IEO it lasts several minutes or even seconds. (5) Investor returns are higher: The value of a listed token is greater than in primary distribution. (6) There is no need to start another wallet. (7) The investment process is simple: investors need to replenish the balance on the exchange, wait for the token to be sold and place a purchase order. (8) Tokens are traded at the same price. This reduces the likelihood of falling rates for early investors who purchased first.”^[733] (el resaltado es mío).

Con razón señala la doctrinaria rusa que la principal ventaja de las IEOs es el acceso inmediato a una gran lista de potenciales inversores, que ya son clientes del *Exchange* que ofrece el proyecto, lo que permite reducir la inversión en marketing. Además, los *Exchanges* suelen usar su propia moneda nativa, en lugar de Ethereum ^[734]. El hecho de que los *Exchanges* utilicen su propio token nativo tiene beneficios para los emprendedores, y para los inversores, ya que estos tokens propios de los *Exchange* tienen menor volatilidad comparado a si se emitiera un token propio para cada proyecto. Además, el token nativo del *Exchange* es utilizado como un utility token, y su uso crece exponencialmente a medida que se listen nuevos IEOs en un *Exchange* dado.

Durante 2019, los IEOs captaron 1.700 millones de Dólares de inversión, pero solo 4 de 15 proyectos fondeados vía IEOs fueron rentables, y la plataforma más utilizada fue Binance ^[735]. Una importante ventaja de recurrir a un IEO en lugar de ICO, además de las arriba listadas por Myalo, es que la plataforma de *Exchange* que se utilice se ocupa del KYC de los inversores, porque ya son sus clientes ^[736]. A la fecha en que se escribe este Manual, Corea del Sur es el único país que ha emitido unos lineamientos específicos para IEOs, ^[737] pero también analiza una nueva legislación que podría prohibir este tipo de mecanismo de financiamiento ^[738].

3.3.2. Tokenización ^[739]

La tokenización es el proceso de creación en *blockchain* de un token digital que representa un activo real y subyacente (sean activos financieros -acciones, bonos-, sean commodities, sean inmuebles, sean obras de arte, etc.) ^[740].

Todo activo real existente en el mundo *off-chain* puede ser tokenizado, no sólo para almacenar en una *blockchain* datos asociados a su ciclo de vida y otros aspectos, sino también para facilitar transacciones *on-chain* sobre bienes

off-chain que se tokenizan al efecto.

Estos activos *reales* tokenizados deben separarse —a los fines pedagógicos— de otros activos que directamente *nacen digitales* y en *blockchain*, como el caso de Bitcoin, donde no hay un activo real subyacente del cual el activo digital derive su valor, y también de las STOs que “tokenizan” participaciones sociales que no cotizan en mercados autorizados pero que se colocan de manera privada y *on-chain* a inversores privados, existiendo incluso plataformas que, como se ha visto, operan como mercado secundario.

La tokenización ha capturado la atención del sector financiero, ya que puede producir una sensible reducción de costos de transacción al eliminar intermediarios, un aumento en la velocidad de las transacciones, el incremento de transparencia, el incremento de liquidez y promover la inclusión financiera en beneficio de pequeños inversores minoristas gracias al *fractional ownership*.

3.3.2.1. Sus beneficios

Los principales beneficios de la tokenización derivan de la *desintermediación*, sumada a la *automatización* de procesos mediante *Smart Contracts*, lo que puede producir grandes ahorros de tiempo y dinero, en beneficio tanto del emisor como del inversor (y en perjuicio de muchos intermediarios que se vuelven innecesarios). La automatización de los pagos, a su vez, puede eliminar el riesgo de contraparte ^[741], es decir, el riesgo de que la contraparte en una transacción incumpla su obligación.

Por otra parte, la naturaleza distribuida de las *blockchains*, la inmutabilidad de su registro, y la aplicación de criptografía asimétrica aporta resiliencia y seguridad para la emisión de tokens. A esto se suma un incremento de transparencia en relación al emisor *per se* y a los activos involucrados, lo que facilita procesos de auditoría en tanto y en cuanto los oráculos ^[742] sean confiables. Los reguladores, por su parte, pueden tener acceso en tiempo real sobre aspectos o momentos del ciclo de vida del token, facilitando procedimientos de AML-KYC.

Por otro lado, la tokenización *desintermedia* fuertemente el proceso de

comercialización: el vínculo es directo entre el emisor del token y el inversor, quienes a su vez pueden beneficiarse de tenencias fraccionales, al dividirse activos reales en muchos tokens ^[743], lo que permite que inversores minoristas participen en negocios que de otro modo quedarían reservados para inversores institucionales por el significativo monto de inversión requerido. Esto beneficia especialmente a las pequeñas y medianas empresas.

En particular, los beneficios de la tokenización pueden impactar en los siguientes ámbitos:

3.3.2.1.1. Comercialización de valores negociables

La tokenización permite que el inversor sea, *per se*, su propio *broker-dealer*, y las transacciones que realiza son validadas por los otros participantes de la red, actuando ésta como agente de registro y de clearing *per se*, recibiendo a cambio un *fee*, des-intermediándose el proceso de comercialización de valores negociables.

Esto no implica, necesariamente, la desaparición de los *market-makers* en ambientes *on-chain*, i.e. *Exchanges* pero implica, por cierto, que una porción de esta ganancia de eficiencia (i.e., reducción de costos de estructuración) será capturada por el proveedor de la plataforma de tokenización, reteniendo asimismo el rol de ser o crear un mercado secundario para los tokens emitidos.

3.3.2.1.2. Pricing de valores negociables

La OECD sostiene que la mayor transparencia de los mercados tokenizados reduciría la asimetría informativa y mejoraría el proceso de formación de precio de los activos digitales. Esto podría permitir que el precio de ciertos valores negociables tokenizados se convierta, *de facto*, en el precio indicativo del activo subyacente, del mismo modo que ocurre con algunos derivados, utilizados para justipreciar los activos subyacentes (i.e., como ocurre con los contratos de futuro o con ciertos Credit Default Swaps ^[744]).

3.3.2.1.3. *Post-trade*

Las funciones de las cámaras compensadoras, que retienen el riesgo de contraparte de ambas partes en una transacción, asegurando el cumplimiento en caso de default de unas de las partes; o el rol de los agentes de depósito que registran titularidad y transacciones y producen pagos, son funciones clásicas de intermediarios que pueden ser reemplazadas por un solo registro, distribuido, inmutable, actualizado con cada transacción, y que puede ser accedido/editado en tiempo real en cualquier momento si se tienen los permisos necesarios.

Lo expuesto es potenciado exponencialmente con la utilización de *Smart Contracts* para transaccionar pagos de manera automática ^[745], segura y trazable, lo que promueve la incorporación de las DLTs como registros descentralizados de datos sobre transacciones pero que también tienen u ofrecen la potencialidad de actuar como contraparte común a todos los actores, eliminando la necesidad de mantener márgenes de garantía exigidos por las cámaras compensadoras ^[746].

3.3.2.1.4. *Desintermediación relativa*

A pesar del potencial de desintermediación expuesto, OECD considera que en este estadio actual, *blockchain* requerirá igualmente un tercero de confianza en aquellos casos en que exista dualidad de activos reales y digitales ^[747]. Este tercero de confianza debería garantizar: (i) la existencia y cualidad del activo real que subyace y justifica su activo digital, (ii) que sólo existe una única representación digital para un mismo activo real; y (iii) ejerza la custodia del activo real subyacente, y ofrezca un ámbito de resolución de disputas.

3.3.2.2. *Tokenización de Valores Negociables*

La tokenización de valores negociables (participaciones sociales, títulos de

deuda ^[748], cuotapartes, etc.) es el ámbito en el cual más crece la digitalización de activos. En algunos casos, el valor negociable *per se* existe en el mundo real y es digitalizado para facilitar su distribución y comercialización, creando una especie de mercado secundario *on-chain* ^[749]. En otros casos, el valor negociable nace directamente digital, sin existencia *off-chain* ^[750].

En ambos casos, se reemplaza el registro electrónico del valor negociable en libros de agentes centrales de depósito, por un registro distribuido en una *blockchain*, que “des-intermedia” las transacciones y permite automatizar algunos o todos los pasos del ciclo de vida del valor negociable mediante *Smart Contracts*.

A su vez, lentamente comienzan a desarrollarse estándares sobre la codificación de *Smart Contracts* ^[751] vinculados a valores negociables, de modo tal que los distintos actores involucrados no deban realizar una auditoría técnica sobre cada *Smart Contract* vinculado a un valor negociable, lo que facilita la utilización valores negociables digitales.

En efecto, la estandarización de ciertos tipos de *Smart Contracts* puede permitir automatizar procesos clave, y esto ha llamado la atención de la International Swaps and Derivatives Association (ISDA), que desde 2019 viene impulsando la creación de *smart derivatives contracts* que incluyen librerías de cláusulas usuales insertas en contratos derivados que pueden ser automatizadas ^[752].

En otro ámbito, es muy interesante la experiencia del Estado de Delaware, que ha sido pionero en materia de *equity tokenisation*: su legislación societaria permite que cualquier compañía emita acciones tokenizadas, y admite que la titularidad de acciones se acredite mediante el token emitido ^[753]. Se volverá sobre el caso Delaware más abajo en este mismo Capítulo. También es muy interesante la experiencia de *Linq*, una plataforma DLT lanzada por el Nasdaq que permite emitir y negociar acciones de compañías que no cotizan y que son tokenizadas para abaratar costos y aumentar la transparencia ^[754].

Sin dudas, la experiencia más interesante es la suiza SDX ^[755], una plataforma que permite emitir y tranzar activos digitales, y tokenizar valores negociables y hasta obras de arte, permitiendo *atomics settlements*. En Argentina, es destacable la experiencia de sesocio.com, que emitió un token nativo llamado *Inve Coin* que se negocia en su plataforma *Investoland*, según mi conocimiento, el primero de su especie. La compañía argentina es el primer marketplace de inversiones colaborativo de la región. Desde sus inicios, ya fueron financiados más de 120 proyectos en diversos países como Estados Unidos, Chile, Argentina, Suiza e Islandia entre otros, por un total de más de 15 millones de dólares, con inversores de 30 países diferentes. En la plataforma se llevan realizadas más de 500 mil transacciones entre inversiones, pagos de renta y movimientos en la plataforma de trading ^[756].

3.3.2.3. Tokenización: ¿la nueva Securitización?

Se ha definido a la securitización como la operación financiera por medio de la cual se obtiene un activo líquido, tal como títulos valores con oferta pública, a partir de activos ilíquidos (tales como derechos creditorios o derechos de cobro, entre otros) que son aislados en una sociedad o patrimonio de afectación *ad hoc* ^[757].

En rigor, securitizar es financiarse recibiendo el *valor presente* de un flujo de fondos futuros. La fuente productora de flujos puede ser muy variada: a) créditos: hipotecarios, prendarios, personales, venta de bienes, por exportaciones, etc. y b) derechos de cobro: alquileres, cobros de peajes, cuotas de universidades, etc.

En alguna medida, la tokenización puede ser considerada una *forma de securitización*, caracterizada por la emisión de un token en *blockchain* que representa el derecho a un valor futuro derivado de un activo subyacente, cualquiera sea éste. Una y otra transforman bienes ilíquidos en líquidos, pero una es muy costosa y pensada para grandes inversores (securitización), mientras que la otra puede presentar significativas ventajas de costos de estructura y puede ser distribuida a inversores minoristas gracias al *fractional ownership* (tokenización). Las seis décadas de experiencia en

securitizaciones [\[758\]](#) puede beneficiar a las tokenizaciones por venir.

Mientras estas líneas se escriben, la empresa Figure ha realizado la primera securitización inmobiliaria on-chain, como se verá *infra* en § 6.1.7.

3.3.2.4. Tokenización Inmobiliaria

La reforma de 2019 al Código Civil de la Federación Rusa admitió que los derechos y obligaciones puedan representarse en forma digital, con lo que la transferencia de derechos digitales es reconocida y admitida por la ley civil rusa, pero aún no se ha tipificado qué tipo de derechos pueden ser digitalizados [\[759\]](#).

En el ámbito del *real estate*, los rusos admiten la tokenización inmobiliaria con fines de comercialización *on-chain* pero exigen un registro “reflejo o redundante” en el registro público inmobiliario *off-chain* [\[760\]](#).

En Estados Unidos comienzan a verse tokenizaciones de importantes desarrollos inmobiliarios desde 2018 [\[761\]](#), al igual que en Francia desde 2019. El caso francés es interesante al constituir la primera venta tokenizada de un edificio en Europa [\[762\]](#).

3.3.2.5. Riesgos y desafíos

La masificación de la tokenización requiere, previamente, resolver importantes cuestiones tecnológicas [\[763\]](#) y regulatorias [\[764\]](#), y, especialmente, avanzar en una definición legal de los *smarts contracts* y en las formas de auditar el código en ellos embebido, o propender hacia su estandarización.

En efecto, la naturaleza de los activos digitales y de los contratos utilizados para tranzarlos -*Smart Contracts*- es una discusión que lejos está de ser zanjada y recién comienza. ¿Se aplican las reglas *off-chain* de los Derechos Reales y de los Derechos Personales al mundo *on-chain*? ¿Hacen falta nuevas

reglas? A su vez, el registro de activos y contratos en la cadena de bloques, ¿tiene valor probatorio? ¿Puede un registro electrónico ser fuente del derecho real de dominio?

La discusión recién comienza, y es resaltable la opinión de los Ingleses, siempre adelantados en materia de Finanzas, Banca y Seguros, sintetizada en una declaración [\[765\]](#) preparada por un grupo de expertos que reúne a jueces, legisladores, y expertos en tecnología y publicada en Noviembre de 2019, que se analizará en profundidad más abajo en § 3.4.3.3.

En síntesis, la postura inglesa afirma:

- i) los criptoactivos constituyen una propiedad pero no son una cosa;
- ii) no pueden ser físicamente poseídos;
- iii) un criptoactivo *per se* no es un título de dominio legal que permita tranzar sobre el subyacente cediendo el título -p.e., una carta de porte-, pero contractualmente esto puede ser regulado como las partes convengan;
- iv) pueden constituir una garantía en determinadas condiciones;
- v) a los fines de insolvencia, son una propiedad;
- vi) si las partes no acuerdan la legislación aplicable a un criptoactivo, es difícil definir cuál es el punto de conexión aplicable;
- vii) una *blockchain* no puede ser considerada un registro público oficial a menos que la ley lo indique;
- viii) los *Smart Contracts* son vinculantes y exigibles si reúnen las condiciones de cualquier contrato;
- ix) los *Smart Contracts* se interpretan igual que cualquier otro contrato;
- x) la anonimidad o pseudonimidad de los *Smart Contracts* no

es un obstáculo para considerarlos un contrato;

xi) una llave privada equivale a una firma; y

xii) el código humano (*human readable*, o *operating code*) de un *Smart Contract* es *per se* un *Smart Contract*.

Sostiene la OECD que la masificación de la tokenización dependerá de que tres condiciones sean cumplidas: (1) exista un sólido caso de negocio donde las DLTs sean una opción superior *vis-à-vis* las opciones convencionales; (2) exista una ventaja tecnológica *vis-à-vis* las tecnologías actuales; y (3) exista una justificación económica en términos de reducción de costos y ganancias de eficiencia medibles [\[766\]](#).

En hipótesis de masificación de la tokenización, puede aparecer un riesgo de iliquidez en los mercados *off-chain*, ya que la liquidez *puede* migrar hacia los mercados *on-chain* [\[767\]](#) y habilitar estrategias de arbitraje de activos que se tranzan tanto en mercados *off-chain* como en mercados *on-chain*. Este riesgo de iliquidez se compensaría con el hecho que la tokenización puede efectivamente reducir la asimetría informativa, toda vez que los tokens incorporan información sobre el subyacente que permite mejorar el *pricing* de los mismos [\[768\]](#).

Es indudable que la tokenización *puede* cumplir una importante función de inclusión financiera, al permitir a inversores minoristas participar en negocios que normalmente están reservados para inversores institucionales, con un gran beneficio potencial para PYMEs como sujeto y objeto de tokenización y captadoras de estas inversiones. El caso parisino de tokenización inmobiliario es muy ilustrativo y podría indicar el inicio de una tendencia.

Asimismo, la tokenización puede facilitar o aumentar la liquidez de ciertos activos ilíquidos, favoreciendo o facilitando su comercialización.

Lógicamente, los beneficios expuestos dependen de que exista una efectiva reducción de costos y ganancias de eficiencia que *justifiquen* tokenizar un proyecto o un negocio, o utilizarla allí en mercados o sectores donde la

confianza deba ser restaurada o asegurada. Es necesario que Argentina asuma una posición de política pública y regulatoria en torno al fenómeno de la tokenización, para lo cual el tema debiera ser objeto de profundo análisis por parte de la Mesa de Innovación Financiera del Banco Central de la República Argentina ^[769] y del Grupo Fintech de la Comisión Nacional de Valores ^[770].

3.4 *Criptoactivos y Smart Contracts: perspectiva comparada*

Habiéndose analizado en los apartados precedentes las particularidades y vicisitudes de la taxonomía del token, así como distintos casos de uso, procede ahora avanzar con el análisis de su encuadramiento jurídico (i) en tanto activo –i.e, criptoactivo–, y en tanto objeto (ii) de un contrato inteligente.

Para ello, se pasará revista a las posturas tomadas por los países que lideran la materia, con la intención de poder desarrollar una visión panóptica de un fenómeno tan nuevo como dinámico.

3.4.1. *Reino Unido*

El Reino Unido es una plaza muy relevante en términos de *blockchain*, al igual que EE.UU, Singapur, Irlanda, y Rusia: los cinco países representaron el 64% de todas las ICOs entre 2016 y 2019 ^[771]. El Reino Unido e Irlanda capturaron el 8.65% de todas las ICOs en ese período; EE.UU el 9.7%, Singapur el 11.82%, y Rusia el 5.68%. Toda la Unión Europea representó el 28.78% de las ICOs ^[772]. El modelo seguido por el Reino Unido en la materia ha sido muy exitoso y seguido por muchos otros países, como se verá seguidamente.

Se ha señalado que cada vez que ha aparecido una nueva tecnología, los Abogados han tendido en general a tomar dos enfoques: (i) uno que favorece la coherencia, entendida como las normas, principios y categorías legales *precedentes*, y en donde el análisis gira en torno a cómo una nueva tecnología

encaja en tales normas, principios y categorías *preexistentes*, con una lógica propia de un Juez o de un abogado litigante; y (ii) otro que favorece la regulación *instrumental*, donde el análisis gira en torno a si las normas, principios y categorías legales precedentes *sirven* o son eficientes para regular una nueva tecnología, o si deben crearse nuevas normas, principios y categorías, con una lógica más propia de un Legislador ^[773].

En general, los ingleses han sido siempre muy pragmáticos, y poco dogmáticos. Así, el enfoque de regulación *instrumental* inglés sobresale mundialmente, como un ejemplo de regulación práctica, que se ha manifestado principalmente en las acciones tomadas por la Financial Conduct Authority (FCA).

3.4.1.1. Principio de Neutralidad Tecnológica y FCA Innovate

En 2014, la FCA se enbanderó rápidamente en el principio de neutralidad tecnológica en relación al entorno *blockchain*, y asumió una postura de regulación instrumental:

“We generally take a ‘technology neutral’ approach to regulating financial services and are interested in considering whether there is anything distinctive about DLT which would require us to take a different approach. DLT’s potential, combined with processing speed (the likes of which has not yet been seen), might suggest that aspects of **existing rules may need to be reviewed** in the light of this new technological context.”^[774] (el resaltado es mío)

Desde esa postura, la FCA –con una actitud evidentemente muy distinta a la SEC– decidió explorar los modelos de negocio en *blockchain*, para poder entender mejor a dónde están los riesgos para el mercado, la competencia y los consumidores, y también divisar cuáles son sus verdaderos beneficios. Esta postura se justifica en una declarada intención, muy firme, del Reino Unido de liderar el entorno FinTech mundial, convirtiéndose en un hub que

atraiga innovación, talento e inversión ^[775].

Así, en 2014 decidió implementar una iniciativa que llamó *FCA Innovate*, con la cual se propuso estimular y promover la innovación y la competencia en servicios financieros en *blockchain*:

“We do so by **removing barriers to entry** where desirable and possible through **clarifying regulatory expectations, examining our own rules and processes** and **providing a test environment for the most innovative ideas**. We also help firms compete at scale by seeking to remove international barriers where possible. **We offer Direct Support** through Innovate to businesses that are looking to introduce groundbreaking or significantly different financial products or services to the market. Our Advice Unit **provides regulatory feedback to firms developing automated models to deliver lower-cost advice to consumers**. The **Regulatory Sandbox allows businesses to test innovative products, services, business models and delivery mechanisms**. Through our RegTech work we **explore how regulatory requirements and technology can align through regulatory technology**. In addition to supporting individual innovative businesses, **we look to add more flexibility to our regulatory framework and identify barriers to entry for innovative firms**. By reviewing our regulatory approach we aim to encourage and support innovation, providing it will not erode consumer protection or the integrity of the financial system.”^[776] (el resaltado es mío)

Desde su lanzamiento hasta Abril de 2019, la FCA recibió 1.600 solicitudes pidiendo apoyo regulatorio ^[777], y acompañó a 700 empresas con modelos de negocio innovadores ^[778], focalizándose incluso en aquellas que ofrecen servicios automatizados de asesoramiento financiero –i.e., *RoboAdvisors* ^[779].

Se han otorgado cerca de 100 autorizaciones para testear nuevos productos o servicios en el *SandBox* que lanzó en 2016 y que ya transita la quinta cohorte ^[780], y han reducido un 40% el tiempo que transcurre hasta que se obtiene una autorización.

El 80% de las empresas que pasaron por el *SandBox* siguen activas ^[781], habiendo recibido inversiones en el capital por casi 140 millones de Libras. La FCA también promueve activamente la internacionalización, mediante un programa de cooperación que exporta e importa startups cuyos modelos de negocio están validados ^[782]. En esa misma línea en 2019 lanzó la *Global Financial Innovation Network* (GFIN) ^[783], una red que aglutina a 35 reguladores financieros de 21 jurisdicciones –incluida Argentina– ^[784], en la cual se realizará el primer Global Sandbox.

3.4.1.1.1. *Regulatory Sandbox*

De todas las medidas que FCA *Innovate* ofrece, sin dudas el Regulatory Sandbox es la más sobresaliente, un verdadero invento inglés y una lógica consecuencia de su pragmatismo y del enfoque de regulación instrumental.

Se trata de la creación de un ambiente super controlado y transparente, donde pueden testearse nuevos bienes y servicios en *blockchain*, con usuarios y clientes reales, de modo tal que la FCA y la empresa puedan sacar conclusiones sobre la performance de la solución, sus riesgos y sus beneficios, y, principalmente, reducir el *time to market* ^[785] y facilitar a la startup el acceso al financiamiento privado ^[786] para escalar la solución, al contar con un permiso estatal solvente que brinda seguridad a los inversores.

El proceso consta de cuatro etapas: aplicación, autorización, testeo y salida ^[787]. Los criterios para analizar cada aplicación que se presenta giran en torno a la innovación de la propuesta, a su contacto (o no) con sectores regulados, los beneficios para los consumidores, a la justificación de la necesidad de usar el *SandBox* y a la preparación (o no) para entrar a fase de

testeo ^[788]. Conseguida la autorización –que puede demorar unos meses– los tests pueden durar entre 3 y 6 meses ^[789], y en ella se limitan tanto el volumen de operaciones máximo como la cantidad máxima de clientes/usuarios.

Evidentemente, todas las ICOs lanzadas dentro del *SandBox* no sufren ataques de parte de la FCA, como sucede con la SEC en el otro lado del Atlántico ^[790], y de hecho el enfoque inglés le ha permitido retener el 8% del total de las emisiones de ICOs, tal como se indicó más arriba. Además, de las 376 aplicaciones de apoyo o pedidos de permiso para ingresar al *SandBox*, 53 fueron presentadas por empresas fuera del Reino Unido, es decir el 14% del total ^[791]. Solo en 2019, se recibieron 99 aplicaciones para la quinta cohorte del *SandBox* ^[792].

La FCA publica información referida a todos los pedidos de autorización que recibe, qué empresas los han presentado, cuáles son sus modelos de negocio, qué feedback se pudo extraer del experimento, y qué pedidos fueron rechazados, y las razones del rechazo.

Es por todo lo expuesto que se ha sostenido que el *SandBox* es un ejemplo vivo del enfoque de regulación cooperativa, combinado con el de diseño regulatorio: en aquél, las reglas y normas a cumplir son co-creadas entre el regulador y el regulado; en éste, las propuestas de valor de las empresas son diseñadas, *ab initio*, con un ojo puesto en los requerimientos aplicables al negocio de que se trate (banca, salud, etc.) ^[793]. Evidentemente, la actitud de una nueva empresa que decide ingresar a un *SandBox* para validar su propuesta de valor, es bastante distinta a la de una gran empresa establecida como Facebook, cuyo slogan corporativo es “*move fast and break things*”, y que probablemente lanzó Libra sin antes consultar con los reguladores, apostando a que la adopción masiva y rápida de su criptomoneda harían política y prácticamente imposible que los reguladores interviniesen ^[794].

Finalmente, nótese que los norteamericanos tienen un concepto similar al

SandBox, al que llaman *safe harbor* ^[795], y que limita el *legal enforcement* de las regulaciones aplicables, es decir, dispone que las autoridades de aplicación se abstendrán de actuar ante determinados hechos o conductas, en tanto se sigan determinados parámetros de conducta predeterminados en la norma que crea el *safe harbor*.

El *safe harbor* más conocido se implementó en 1996, con la finalidad de blindar a los Internet Service Providers por los contenidos que circulan en Internet ^[796]. Los *safe harbors* tienden a ser permanentes, y no necesariamente benefician a nuevas empresas; mientras que los *SandBoxes* suelen ser temporarios, y están principalmente enfocados en fomentar el emprendimiento y nuevos bienes y servicios ^[797].

3.4.1.1.1.1. Otros países que siguen el modelo *SandBox*

El modelo experimental inglés fue tan exitoso en tan poco tiempo –se lanzó en 2016–, que rápidamente fue imitado por reguladores de otros países: Hong Kong, Malasia, Singapur, Montreal, la Isla de Man, Canadá, Indonesia, el estado de Arizona, Sri Lanka, Australia, Bahrein, Tailandia, Rusia y también por la Unión Europea. También España está en proceso de sancionar una ley que creará un *SandBox* ^[798]. En el caso de Latinoamérica, en 2018 el Banco Interamericano de Desarrollo ha propuesto que se adopte esta metodología a nivel regional ^[799] y México lo ha hecho.

En el caso de Australia, el *SandBox* permite testear nuevos bienes y servicios durante 12 meses sin tener una licencia de servicios financieros ^[800]. En el caso de la Unión Europea, la Comisión Europea ha propuesto a las autoridades competentes de cada Estado Miembro que establezcan *regulatory sandboxes* para promover la innovación ^[801]. Canadá implementó el *SandBox* en 2017, y exige que los candidatos a ingresar al *SandBox* permitan una prueba en vivo del servicio o plataforma, entreguen un plan de negocios y demuestren los potenciales beneficios para los

consumidores ^[802].

3.4.1.2. Lineamientos de la FCA sobre criptoactivos

El principio de neutralidad tecnológica y el enfoque de regulación instrumental de la FCA no significa que la misma no tome posición respecto a los *hot topics* del entorno *blockchain*.

En efecto, en Julio de 2019, la FCA emitió sus lineamientos sobre criptoactivos ^[803] en donde definió tres tipos de tokens: exchange tokens ^[804], utility tokens ^[805] y security tokens ^[806], y declaró que su poder de policía se restringe normalmente a los security tokens en función de lo previsto en la Ley de Servicios Financieros y Mercados del año 2000 ^[807], y solo excepcionalmente a los utility tokens, en tanto y en cuanto puedan ser considerados dinero electrónico ^[808], como es el caso de algunas StableCoins ^[809].

La FCA consideró entonces que los security tokens sí caen dentro del poder de policía de la FCA ^[810], y también analizó los tokens duales o *híbridos*, aquellos que a lo largo de su ciclo de vida, van cambiando de naturaleza. Al respecto, sostuvo:

“We know that tokens can move between categories during their lifecycle, and sometimes work in tandem with other tokens during the launch of a new network. In either case, **the regulatory treatment depends on the token’s intrinsic structure, the rights attached to the tokens and how they are used in practice.** If the token at a point in time reaches the definition of an e-money token or a security token, then it will fall under regulation ^[811]” (el resaltado es mío)

Finalmente, la FCA también abordó los *Airdrops*, del siguiente modo:

“Airdrops refers to the distribution of tokens, usually for free, to consumers. They are primarily used by new networks to attract more users but have also been used by existing networks to get additional users or generate further attention...**A specified investment is not contingent on it being purchased for value**, and a token can be a security token even if nothing is received for it.”^[812] (El resaltado es mío)

3.4.1.3. *LawTech Delivery Panel y la UK Jurisdiction Taskforce (UKJT)*

Como una de las iniciativas de la alianza público-privada TechNation creada en 2015 en el Reino Unido^[813], se formó el denominado LawTech Delivery Panel, con el objeto de transformar al sector legal inglés con apoyo financiero del Ministerio de Justicia^[814]. Uno de los grupos de trabajo del LawTech Delivery Panel es el UK Jurisdiction Taskforce (UKJT), formado por abogados, jueces, reguladores, emprendedores y gobiernos^[815].

Luego de las *Guidelines* emitidas en Julio de 2019 por la FCA, en Noviembre del mismo año la UKJT emitió una interesante Declaración en relación a los criptoactivos y los contratos inteligentes que amerita detenimiento y profundo análisis. Antes de ello, debe puntualizarse que la UKJT no duda en afirmar que los criptoactivos y los contratos inteligentes representan el futuro^[816], y que los tópicos tratados en la Declaración serán tarde o temprano sometidos a decisiones judiciales, aspirándose a que los puntos desarrollados en su Declaración *sirvan para dar claridad a cuestiones legales críticas*.

3.4.1.3.1. *Características de los criptoactivos*

3.4.1.3.1.1. *Autenticación vía encriptación*

Los criptoactivos se representan funcionalmente por dos parámetros, uno público (llave pública) y otro privado (llave privada). La llave pública contiene información sobre el criptoactivo, i.e., su propiedad, su valor y su historial de transacciones. La llave privada permite su transferencia, mediante una firma digital criptográfica, con lo cual la llave privada es la que confiere el control sobre el activo.

Algunos criptoactivos operan con *varias* llaves privadas, i.e., *multisig*, con lo que varias personas controlan un mismo activo [\[817\]](#). A su vez, una persona puede acceder a la llave privada de un criptoactivo por distintas razones: (i) por cuenta y orden de otro, en cuyo caso reconoce la propiedad en un tercero y existe una relación contractual subyacente; o (ii) por medios ilegales, con lo cual no es un dueño legítimo. Finalmente, identificar al dueño de un criptoactivo puede ser difícil por la anonimidad y pseudonimidad de las *blockchains* públicas [\[818\]](#).

3.4.1.3.1.2. Uso de un registro distribuido de transacciones

Se abordó en la Declaración de la UKJT si el uso de una DLT puede equipararse a un registro público con fines legales constitutivos o declarativos. Se considera que sólo si una ley expresamente reconoce tales funciones, entonces la DLT tendría tales efectos legales.

3.4.1.3.1.3. Protocolo de gobierno

Las reglas de consenso o protocolos de gobierno, tales como PoW o PoS, son las que determinan cuál versión del registro distribuido es la correcta. Sólo las transacciones que cumplen con estos protocolos auto-ejecutables se agregan al registro distribuido y descentralizado [\[819\]](#).

3.4.1.3.1.4. Transferencia vs. Gasto & Doble Gasto

Las transferencias de criptoactivos i.e. su gasto, se transmiten a una red de

participantes para que las confirmen y las agreguen al registro digital de transacciones. Esto busca evitar que se realicen dos transferencias inconsistentes sobre un mismo criptoactivo ^[820]. Cuando se transfiere un criptoactivo, esto es lo que ocurre:

“the transferor typically brings into existence a new cryptoasset, with a new pair of data parameters: a new or modified public parameter and a new private key. **The data representing the “old” cryptoasset persists in the network, but it ceases to have any value or function because the cryptoasset is treated by the consensus as spent or cancelled so that any further dealings in it would be rejected.** The “new” cryptoasset is represented by new data and controlled by a new key. There is a closer analogy with a bank payment where no property in the payer’s funds passes to the payee; instead new property is created by the credit to the payee’s account. A transfer is completed, and a new cryptoasset is created, once the transferor authenticates and broadcasts it. It may take some time for a transaction to be entered onto the ledger and accepted by the consensus but in principle that should not prevent or delay the transferee’s assumption of ownership of the cryptoasset. As we explain below, the ledger should not be regarded as a definitive record of title. **However, until the transaction is on the ledger, there is a risk that the transferor will make a second transfer (i.e. double-spending the cryptoasset) and that that will be accepted on the ledger in priority to the first.** The (first) transferee’s cryptoasset would then not be recognised as validly transferred and so would in practice be worthless ^[821].” (El resaltado es mío)

3.4.1.3.1.5. *Son una propiedad*

La Declaración de la UKJT afirma que los criptoactivos son una propiedad

para el Derecho Inglés, y esta naturaleza no se modifica por el hecho de que sean “pura información [\[822\]](#)”, sin sustrato físico [\[823\]](#).

Al ser una propiedad, le son aplicables las reglas que rigen la sucesión de las personas y el desapoderamiento en casos de insolvencia, al igual que las reglas sobre fraude, robo y administración fraudulenta [\[824\]](#). Al ser puramente “virtuales” o “digitales”, no pueden ser poseídos físicamente, con lo cual no pueden ser dados en depósito, aunque quizás podrían ser objeto de ciertos derechos reales o personales de garantía.

Señala la UKJT que el Derecho Inglés debiera aplicarse en transacciones con criptoactivos si: (i) algún activo off-chain relevante a la transacción está situado en el Reino Unido; (ii) existe algún control centralizado en el Reino Unido, i.e. en casos de *blockchains* privadas; (iii) un criptoactivo está controlado por alguien en el Reino Unido, i.e., por poseer la llave privada; y (iv) si las partes eligen el Derecho Inglés.

3.4.1.3.1.6. Criptoactivo como garantía convencional

La UKJT también aborda la posibilidad de utilizar criptoactivos para constituir una garantía a favor de un tercero [\[825\]](#), y concluyen que es posible constituirlos, pero sólo en las tipologías en las cuales no es necesario transferir la posesión al acreedor garantizado.

3.4.1.3.1.7. Criptoactivos vinculados a bienes off-chain

Finalmente, la UKJT también analiza el caso de ciertos criptoactivos que están vinculados a bienes off-chain, y qué ocurre cuando uno o ambos son transferidos. Está claro que si ambos bienes, i.e. el criptoactivo y el activo físico, son objeto de un contrato entre las mismas partes, será el contrato el que fije las consecuencias legales y las formas de transferirlos. El escenario más complejo es el que vincula a terceros que alegan derechos sobre los bienes off-chain, desconociendo quizás el vínculo que exista entre dicho bien y un criptoactivo [\[826\]](#).

3.4.1.3.2. *Smart Contracts*

La UKJT también abordó la naturaleza jurídica de los contratos inteligentes, a los que no duda en considerar contratos con efectos legales. En lugar de intentar definirlos, se puntualizó su característica más sobresaliente: su automaticidad, la que se describe en estos términos:

“a Smart Contract is performed, at least in part, automatically and without the need for, and in some cases without the possibility of, human intervention. That requires the terms of the contract to be recorded in computer-readable form, i.e. in code. [\[827\]](#)”

3.4.1.3.2.1. *La forma de los contratos en el Derecho Inglés. Interpretación de un contrato*

Se puntualiza en primer término que el Derecho Inglés no requiere normalmente una determinada forma contractual [\[828\]](#), y reconoce la existencia de un contrato si se cumplen los tres requisitos a ellos impuestos [\[829\]](#).

Con relación a la exigencia de forma escrita, y a la representación de un contrato a través de lenguajes de programación, se afirma que el código del contrato puede ser considerado lenguaje escrito, tanto en versión de código fuente –legible por humanos– como *object code* [\[830\]](#), y por ende, cumple el requisito de forma escrita para un contrato [\[831\]](#). Esto no cambia por el hecho de ser un lenguaje desconocido; la situación es equivalente a la de un idioma extranjero. Existen traductores.

En punto a la interpretación de un contrato inteligente, se sostiene:

“At first blush, a Smart Contract that exists purely in code is not susceptible to the exercise of contractual interpretation at all, in part because interpretation is about ascribing meaning to natural language, and in part because code is generally clear, unambiguous and self-consistent (albeit that is not always the case, as discussed below) ...That is not because there is anything special about such a Smart Contract. Rather, it reflects the entirely conventional position that where language is clear and unambiguous (which code generally is), it would require very unusual circumstances for a judge to conclude that the objective meaning was other than what the words (code) said... however, there will likely also be **cases where examination of the code alone will not be sufficient to ascertain contractual intention** and, just as with natural language contracts, a judge will need to look beyond the four corners of the code to interpret it....Where there is code involved, part of that exercise will be a determination of whether the **code (or part of it) was intended to define the obligations or whether it was intended merely to implement them**. In the former case, an investigation of what the code actually does (possibly with the assistance of expert evidence) may be needed as part of the exercise of interpretation. Where a Smart Contract subsists solely in code, and where that code is unambiguous, the judge may well need to do no more than decide that the parties intend to be bound by the code—whatever it does. Where the code contains ambiguities, or where a contract consists both of code and natural language (where the court may need to understand how the two fit together) extrinsic evidence is likely to be needed. **Where code merely implements an agreement, the question of what the code actually does will be irrelevant to interpretation**; but investigation of the code may still be necessary if a dispute has arisen as to whether the code correctly implements the agreement”^[832] (el resaltado es mío)

Se analizó también si la llave pública o privada equivale a una firma

electrónica, y se concluye que firmar a través de una llave privada es una forma más de firma electrónica [\[833\]](#).

3.4.2. Estados Unidos de Norteamérica

La situación de la *blockchain*, los criptoactivos y de los contratos inteligentes en EE.UU amerita distintos enfoques, en función del carácter federal del país y la gran autonomía que tienen los Estados que conforman la unión.

3.4.2.1. Empresas que operan criptoactivos

En primer término, para intentar armonizar la legislación estadual, en 2017 se ha propuesto una Ley Modelo para empresas que operan con criptoactivos [\[834\]](#), en la que se definen pautas de protección para los consumidores, actividades exentas, actividades que deben registrarse, y actividades que están sujetas a una licencia previa.

La ley modelo no regula a las monedas virtuales *per se* aunque sí las define [\[835\]](#), sino que regula la actividad comercial y servicios ofrecidos para el intercambio de monedas digitales [\[836\]](#), la transferencia de monedas digitales, y servicios de depósito de criptomonedas [\[837\]](#).

La ley prevé un *SandBox* y establece ciertos niveles de reservas exigibles a empresas que ofrecen servicios de depósito de criptomonedas [\[838\]](#). Los Estados de Hawaii [\[839\]](#), Nebraska, California, Nevada, Rhode Island y Oklahoma han aprobado o analizan aprobar leyes que siguen esta ley modelo. Por su parte, el Estado de Florida ha sancionado una ley definiendo “criptomonedas” a los fines de su legislación antilavado [\[840\]](#) y por ley creó un grupo de trabajo para estudiar los beneficios de la *blockchain* [\[841\]](#).

3.4.2.2. Admisión y utilización de la blockchain a nivel federal y estadual

Señala Arcari^[842] que a Abril de 2019 se habían introducido 133 proyectos de ley a nivel Estadual, que regulaban el uso de la *blockchain* en alguna medida, incluyendo 5 proyectos de ley que regulan específicamente a los contratos inteligentes^[843].

En 2018 también se ha propuesto una Ley federal de Promoción de la *Blockchain*, que aún sigue su curso en el Congreso^[844], por la cual se propone crear, en el ámbito de la Secretaría de Comercio, un Grupo de Trabajo en *Blockchain* compuesto por representantes de las agencias federales, empresas de tecnología, representantes de todos los sectores industriales, representantes de las PyMES, investigadores, ONGs y representantes de los sectores rurales. El Grupo de Trabajo debiera elaborar un informe dentro del plazo de un año, indicando los usos potenciales de la *blockchain* a nivel del Gobierno Federal y de todos los sectores del comercio.

También puntualiza Arcari^[845] que muchos doctrinarios^[846] e incluso la prestigiosa CHAMBER OF DIGITAL COMMERCE^[847] sostienen que dos leyes federales preexistentes alcanzan y sobran para regular la *blockchain* y los contratos inteligentes a nivel estadual: la *Electronic Signatures in Global and National Commerce Act* (Ley E-SIGN) y la *Uniform Electronic Transactions Act* (Ley UETA).

3.4.2.2.1. Admisión expresa de los contratos inteligentes a nivel estadual

En 2017 Arizona se convirtió en el primer estado del Mundo en regular los contratos inteligentes^[848], reconociéndoles carácter legal y vinculante. La ley definió a la *blockchain*^[849], y modificó la ley provincial de transacciones electrónicas, de modo tal de incluir en ésta a la *blockchain* y a los contratos inteligentes, considerándose que el requisito de firma electrónica se cumple

también mediante *blockchain* y las llaves públicas y privadas ^[850]. Arcari señala que la definición de contrato inteligente es lo suficientemente amplia como para incluir criptomonedas, hipotecas, títulos valores, y otros bienes tranzables tokenizables ^[851].

Nevada también sancionó un paquete de cuatro ^[852] leyes, una de las cuales admite los contratos inteligentes ^[853], otra incluye un *SandBox* ^[854], otra admite los registros de una *blockchain* y prohíbe cobrar tasas adicionales por el uso de dicha tecnología ^[855], y una cuarta define a las criptomonedas ^[856]. En 2018, Tennessee también sancionó una ley ^[857] en la que reconoce la fuerza legal de los *Smart Contracts*.

Finalmente, el Estado de Nueva York ^[858], por su parte, en 2014 fue el primero en regular el *trading* de criptomonedas con su controvertida BitLicense ^[859], que produjo un éxodo masivo de empresas enfocadas en *blockchain* ^[860]: Luego, en línea con la ley de Arizona presentó un paquete de cuatro leyes ^[861] vinculadas a *blockchain*, admitiendo y definiendo expresamente los contratos inteligentes ^[862], creando un grupo de trabajo para analizar la implementación de *blockchain* a nivel estatal y el impacto de las criptomonedas, y también ordenando el estudio de la viabilidad de la *blockchain* en procesos electorarios ^[863].

3.4.2.2.2. Regulación de la *blockchain* a nivel estadual

Vermont fue el primer estado en regular, en general, la *blockchain* en 2015 ^[864], y tres años después, en 2018 sancionó una muy novedosa ley ^[865] que creó las *Blockchain-based Limited Liability Company* (BLLCs). Las BLLCs pueden funcionar orgánicamente en *blockchain*, incluyendo las votaciones y todas las decisiones orgánicas, y permiten la utilización de *Smart Contracts* del modo en que los socios lo dispongan, pero su formación no la

exime de cumplir con las leyes estatales y federales que gobiernan la emisión de títulos valores.

En 2016, Delaware lanzó la *Delaware Blockchain Initiative* (DBI) ^[866] e Illinois hizo lo mismo en 2017 ^[867]. El caso de Delaware es muy importante, ya que es una plaza muy relevante en materia societaria a nivel nacional: en Delaware están inscriptas el 66% de las empresas Fortune 500 y el 85% de todas las sociedades que lanzan IPOs ^[868].

Poco tiempo después, en 2017 se sancionó una ley que permite tokenizar participaciones sociales de sociedades constituidas en Delaware que no cotizan, con intención de llevar un registro *on-chain* de las emisiones y de sus transferencias ^[869]. El 11 de Junio de 2018 se emitían las primeras acciones tokenizadas en la *blockchain* de Ethereum, como consecuencia de la DBI ^[870], en un modelo muy interesante de RegTech ^[871]. La nueva legislación propuesta por la DBI también permite que ciertos registros de créditos comerciales garantizados se gestionen, tramiten y obtengan vía *blockchain* ^[872].

El Estado de Illinois, por su parte, sancionó una ley sobre *blockchain* y *Smart Contracts* que entró en vigor en Enero de 2020 ^[873], quizás la más completa de todas las leyes estatales, y en la cual expresamente se reconoce validez y fuerza legal a los contratos inteligentes en varios supuestos ^[874], aunque no en todos los casos ^[875]. También en Illinois se implementó un muy interesante proyecto piloto para migrar el registro inmobiliario a *blockchain* con el apoyo de la INTERNATIONAL BLOCKCHAIN REAL ESTATE ASSOCIATION ^[876].

En 2019, el Estado de Wyoming tomó la posta en la iniciativa legislativa subnacional, desplazando incluso a Delaware, y sancionó un enorme paquete de trece leyes ^[877], convirtiéndose en la plaza más *crypto-friendly* en EE.UU.

El amplio paquete legislativo recepta la *blockchain*, definiendo a los criptoactivos, incluyendo a los *utility* o *consumer* tokens –fue el primer

Estado en reconocer los *digital consumer assets*–^[878], a las llaves privadas, a los acuerdos de firma múltiple –i.e., *multiSig*, y definiendo y admitiendo el uso de *Smart Contracts*^[879]. También permite emitir *certificate* tokens que representan participaciones sociales, es decir, admite expresamente la tokenización de acciones. Además, la legislación de Wyoming creó un *SandBox*, y hasta una licencia especial para bancos de Wyoming que quieran comenzar a operar con criptoactivos, pudiendo sólo actuar solo como depositarios pero no pudiendo realizar préstamos, es decir, no pueden realizar intermediación financiera con criptoactivos y deben mantener el 100% de los criptoactivos en sus reservas^[880]. También autorizó a las empresas de minería que se instalen en Wyoming a negociar tarifas eléctricas directamente con los productores de energía mediante una modalidad contractual específica^[881], sosteniéndose incluso que los precios de la energía con fines de minería serían los más bajos del mundo^[882].

El caso de Wyoming es trascendente ya que ha manifestado una tendencia legislativa estadual que se ha bifurcado en EE.UU: por un lado, están los estados que siguen las propuestas de la Uniform Law Commission –el más importante siendo California^[883]–, y por el otro lado, Wyoming y los estados que siguen su postura^[884]. El punto en discusión es muy relevante: la propuesta de ley suplemental^[885] uniforme elaborada por la Uniform Law Commission modifica la Ley modelo analizada más arriba en § 3.4.2.1., y, se alega, estaría fuertemente sesgada *a favor* de los intermediarios de títulos valores, los brokers, estructuradores, etc^[886]. En este sentido, se ha sostenido que el enfoque de Wyoming es el correcto y el de la Uniform Law Commission es el incorrecto, en estos términos:

“The Uniform Law Commission’s use of the Article 8 indirect ownership regime for digital assets renders their proposed Model Acts unworkable because it not only **perpetuates the same flawed system for digital assets, it makes things worse.**

As the founding director of the Delaware Blockchain Initiative, I cannot stay silent about a law that **would extinguish the power of blockchain technology to clean up problems in capital markets**. Unfortunately, by mandating indirect ownership treatment for virtual currencies, I fear that's what the Model Acts would do. [\[887\]](#)” (el resaltado es mío)

Por otro lado, en el Estado de Colorado entró en vigor en Agosto de 2019 una interesante ley [\[888\]](#), que expresamente aborda la taxonomía de los tokens, y crea excepciones específicas para quienes emiten utility tokens con fines de uso o consumo de bienes o servicios digitales, diferenciándolos expresamente de los security tokens, siguiendo el criterio de Wyoming [\[889\]](#).

Otro muy interesante proyecto de ley en Colorado propone estudiar la aplicación de la *blockchain* en el sector agropecuario [\[890\]](#), con el fin de dar mayor trazabilidad a la producción, llevar un control de inventarios, monitorear condiciones climáticas, implementar un archivo sobre equipamiento de producción y transporte, verificar el origen de determinados productos y certificarlo, trazabilidad de fertilizantes y semillas, y el intercambio de activos.

Similar camino ha transitado el Estado de Montana, que sancionó legislación para excluir a los utility tokens de toda la la normativa aplicable a los security tokens en tanto tengan una preponderante finalidad de consumo y ésta esté operativo a más tardar dentro de los 180 días siguientes a la venta de los tokens, prohibiendo a los compradores su reventa hasta tanto su finalidad sea funcional, es decir, puedan permitir el acceso, uso o consumo de los bienes o servicios digitales que son su objeto [\[891\]](#).

3.4.2.2.3. *The Crypto-currency Act of 2020*

En marzo de de 2020, un congresista de Arizona [\[892\]](#) presentó al Congreso de EE.UU un proyecto de ley conocido como la *Crypto-currency Act* de

2020^[893], con la intención de clarificar los poderes regulatorios de las agencias federales.

El proyecto propone tres clases de activos digitales: cripto-commodity^[894], cripto-moneda^[895], y cripto-security^[896] y reparte el poder de policía entre la Commodity Futures Trading Commission (CFTC), la Secretario del Tesoro, y la SEC, respectivamente. También define a los *Smart Contracts*^[897], a los Oráculos^[898], y dos tipos de StableCoins^[899].

3.4.3. Singapur

El caso de Singapur merece su atención, ya que fue uno de los primeros países en abordar en profundidad la taxonomía del token, lo que a su turno lo convirtió en una plaza muy atractiva para emisiones, atrayendo casi el 12% de todas las ICOs creadas entre 2016 y 2019^[900].

La Autoridad Monetaria de Singapur (MAS, en inglés) publicó unos *Lineamientos* sobre el ofrecimiento de tokens digitales en 2018^[901] que se analizan en profundidad a continuación.

3.4.3.1. Tokens regulados

La Autoridad Monetaria afirma que los tokens que sean productos del mercado de capitales están regulados por la *Securities and Futures Act*. Para determinar si un token cae dentro de la regulación, se analizan los derechos que contiene. Generalmente quedan comprendidos los tokens que representen participaciones en el capital en personas jurídicas, debentures, participaciones en fideicomisos, contratos derivados donde el activo subyacente es alguno de los anteriores supuestos, o una participación en esquemas de inversión colectivos, o una opción para adquirir una participación^[902].

Existen ciertas excepciones para emitir tokens regulados, cuando se hacen ofertas personales de menos de 5 millones, o sin oferta pública, o se dirigen a

inversores institucionales o inversores acreditados ^[903]. La Autoridad de Singapur también dispone las licencias que deben solicitar las plataformas de emisión primaria, los asesores financieros, y las plataformas de *trading* ^[904].

3.4.3.2. Tokens no regulados. SandBox

Los Lineamientos sobre el ofrecimiento de tokens digitales también incluyen una serie de ejemplos ilustrativos de tokens que quedan fuera de su poder de policía, i.e., utility tokens. Asimismo, si el token fuera regulado, es posible aplicar para un *SandBox*.

3.4.4. Suiza

3.4.4.1. FINMA

Como se adelantó ^[905], Suiza también adoptó un rápido posicionamiento sobre los criptoactivos en 2017 y 2018.

En 2017 emitió un documento donde describía el tratamiento de las ICOs ^[906], sobre la base del principio de neutralidad tecnológica y se afirmaba la aplicación de las normas de KYC-AML para ICOs e intermediarios que involucren, como los *Exchanges*, instrumentos de pagos ^[907].

A su vez, FINMA indicaba que (i) aceptar depósitos que generan una obligación a favor del comprador del token podía quedar sujeto a regulaciones bancarias ^[908]; (ii) la emisión de tokens que fueran considerados securities requería una licencia previa ^[909] y (iii) ciertos esquemas de inversión colectiva estaban también regulados ^[910].

Simultáneamente, FINMA tomó acciones contra emisores de ICOs

fraudulentas, como el caso de *E-Coins*, una supuesta moneda estable descentralizada, liquidando sociedades en infracción ^[911] y, además, publica y actualiza una lista de ICOs posiblemente fraudulentas ^[912].

En 2018, FINMA publicó unas nuevas *Directrices* sobre ICOs ^[913], definiendo la información que debía presentarse para solicitar algún tipo de licencia y definiendo un enfoque casuístico pero holístico y basado en la realidad económica a la hora de evaluar cada ICO ^[914].

Estas *Directrices* clasificaron los tokens digitales en cuatro especies: (i) payment tokens ^[915], (ii) utility tokens ^[916], (iii) asset tokens ^[917], y (iv) *hybrid* tokens ^[918]. A su vez, se definieron dos formas de creación de tokens: *pre-financing* ^[919] o *pre-sale* ^[920]. Específicamente con relación a los payment y utility tokens, FINMA fijó posición en no considerarlos un título valor regulado ^[921], pero en cambio, respecto a los asset tokens, FINMA fijó el criterio de considerarlos un título valor regulado ^[922], y en éstos casos existen licencias obligatorias previas y otras obligaciones de hacer aplicables ^[923].

Finalmente, en 2019 FINMA emitió también unos lineamientos específicos para *StableCoins* ^[924], reafirmando el principio de *substance over forms*, y sosteniendo que aplicará en general el principio de *same risks, same rules*, al abordar cada caso en particular.

Clasificó las monedas estables en cuatro categorías: (i) vinculadas a monedas *fiat* ^[925]; (ii) vinculadas a commodities ^[926]; (iii) vinculadas a activos inmobiliarios ^[927]; y (iv) vinculadas a títulos valores ^[928].

3.4.4.2. *La Swiss LegalTech Association (SLTA): su posicionamiento en contratos inteligentes*

Puntualmente en relación a los contratos inteligentes, debe resaltarse el trabajo impulsado por la Asociación Suiza de LegalTech ^[929]. Los criterios y reflexiones de la SLTA son muy importantes para la República Argentina, ya que la influencia del Código Suizo de las Obligaciones ha sido, directa o indirectamente, muy relevante en la legislación argentina ^[930]. En este sentido, la SLTA define a los contratos inteligentes y su funcionalidad y también precisa sus limitaciones ^[931]:

“a program code in which terms of a contract are reproduced and digitally linked to cryptocurrency or other digitally stored information. This program code is stored in a decentralized ledger infrastructure, a public or a private blockchain, which leads to the main characteristics of a Smart Contract: Self-enforceability and Immutability...for most real-world applications, there has to be the ability to access and/or otherwise interact with external data (e.g., IoT platforms, management systems or web services, and/or APIs), in order to execute the given program code and instructions autonomously. This external information sources (typically referred to as “oracles”) have to be available in a machine-readable form (although manual intervention “oracles” may be envisaged, the resulting instruction from such oracle will need to be in a predetermined format which the Smart Contract code is capable of computing). Therefore, with the access to the relevant data, a Smart Contract can be described as a data driven self-executing code.” ^[932]

También se puntualiza que, al igual que en la vida real –i.e., *off-chain*–, los contratos inteligentes pueden ser pre-redactados por una de las partes:

“Like in the real world, it is perfectly possible for only one party

to define conditions in a Smart Contract and publish the same on a blockchain. In a sense, this serves as an offer to the public to enter into an agreement on the terms programmed in the Smart Contract. No legal contract is originated then so far. However, when a party fulfills the conditions of the Smart Contract (e.g. by paying an amount of Bitcoin to a specified address), this act is deemed to be the acceptance of the offer, so that both parties accept the conditions and, presumably, a legal contract is originated corresponding to the conditions written in the program code (subject to applicable law, etc.). No intermediaries are needed and the transaction is stored and cryptographically secured on a blockchain. All parties can be sure that execution will happen when the predefined conditions are fulfilled. In summary, a Smart Contract which incorporates the execution of the terms of a transaction among two parties will always have an underlying legal contract (in writing or just verbal). It is the connecting interface between the agreements of the mutual assent of the contract parties' and the execution of the terms. Contracting parties can be sure that the agreement will be executed in the way it is fixed in the program code. To make that autonomous execution possible, all information in terms of defined conditions has to be available for the program code. That being said, a Smart Contract possibly needs access to external data outside of a blockchain, such as inputs from IoT platforms, management systems or web services, to execute the given agreements fast and autonomous ^[933]”.

Respecto al encuadramiento y reconocimiento de los contratos inteligentes de acuerdo al derecho nacional Suizo, se puntualiza que:

“In the blockchain world, a Smart Contract is a program written by a user in order to carry out a transaction with other users on the blockchain, who accept the terms of that transaction. **A Smart Contract can thus be legally assimilated**

to an accepted offer and therefore, to a contract. However, the essential elements of the proposed contract must be clearly spell out in the program, be sufficiently precise, clear and understandable to be validly accepted by all parties. [\[934\]](#)” (El resaltado es mío).

Además, la SLTA, afirma que, si se considera que un *Smart Contract* publicado en la *blockchain* es una oferta a contratar, también se puede perfeccionar un contrato bajo la legislación suiza atendiendo a las acciones y conductas posteriores de las partes, que permiten que una parte *tácitamente* acepte una oferta [\[935\]](#). La conducta de las partes puede y debe ser interpretada de acuerdo al principio de buena fe y atendiendo a todas las circunstancias del caso [\[936\]](#), siempre que se trate de un contrato que no requiere una forma determinada para su celebración. Aún para éstos casos – contratos formales–, la SLTA afirma que:

“some contracts are required by law to be in writing and thus would not be valid under Swiss law if they were only registered in the blockchain. However, there is the possibility to use qualified electronic signature as defined by the Federal Act of December 19 2003 on Electronic Signature, **which is deemed equivalent to a handwritten signature**. It is indeed possible to link a document within the blockchain via a timestamped hash. [\[937\]](#)” (el resaltado es mío)

Pero, si el contrato es formal y, además, requiere su registro en algún registro público, entonces:

“it seems hardly difficult to have it translated into a Smart Contract in the current legal system, as it requires an entry in the public register done by a public notary. Two individuals would not be able for example to proceed to the sale of an

immovable property through a Smart Contract without a formal deed acknowledged by a notary. [\[938\]](#),”

Con relación a la prueba del contrato ante un eventual litigio, sostiene la SLTA que:

“The Swiss Supreme Court ruled that **an email where the content was sufficiently precise and clear was deemed an offer and a contract was formed by the acceptance of the offer by the other party.** Thus, the acceptance by the judge of the validity an “electronic” contract should also apply to Smart Contract. [\[939\]](#)” (el resaltado es mío)

También se analizan cuestiones vinculadas a la capacidad para contratar [\[940\]](#), errores de programación [\[941\]](#), modificaciones contractuales [\[942\]](#), objetos contractuales ilegales [\[943\]](#) y la cuestión muy sensible de la anonimidad o pseudonimidad [\[944\]](#).

Finalmente, pero no menos importante, se diferencia adecuadamente entre *smart legal contracts* [\[945\]](#) y *Smart Contract code* [\[946\]](#) y concluyen afirmando que no es necesario modificar el régimen legal Suizo para reconocer validez legal a un *Smart Contract* [\[947\]](#).

3.4.5. España

Autorizada doctrina ha sostenido que los contratos inteligentes son acuerdos productores de efectos jurídicos cuya peculiaridad esencial es que son “autoejecutables” por estar total o parcialmente recogidos en secuencias de código: la ejecución del contenido no depende de la voluntad de las partes, sino que tiene lugar de manera automática, una vez se dan las condiciones

preestablecidas por aquéllas [\[948\]](#).

Por tanto, no todas las cláusulas de un contrato convencional podrán ser objeto de codificación, ya que, por ejemplo, aquéllas cláusulas que necesiten de interpretación para ser verificadas –buena fe, consumidor medio, diligencia debida, interés superior del menor, etc.–, no tendrán cabida, al igual que conceptos como “caso fortuito” o “fuerza mayor”. Por tal motivo, se afirma que los *Smart Contracts* serán más frecuentes en el ámbito de los contratos de suministro, la fabricación de productos, o el intercambio de bienes por dinero, entre otros [\[949\]](#).

Antes de iniciar el análisis de la legislación española, merece traerse a colación un trabajo de la CHAMBER OF DIGITAL COMMERCE de EE.UU [\[950\]](#) que analizó el caso puntual de los contratos inteligentes en la legislación española vis-à-vis los requisitos que los contratos deben cumplir para ser legalmente válidos. Se concluyó que en España no hay obstáculo alguno para que un *Smart Contract* sea un contrato en sentido legal, vinculante y exigible, y que incluso las partes pueden actuar pseudónimamente cuando actúan a través de un mandatario [\[951\]](#), aunque lo recomendable (i.e., lo necesario) sería asegurar la identidad de la persona que celebra un contrato inteligente a través de algún mecanismo *off-chain* [\[952\]](#).

3.4.5.1. Legislación aplicable

Siguiendo la sobresaliente exposición de Legerén-Molina, afirma que en España no existe una legislación específica sobre contratos inteligentes, siéndoles de aplicación la normativa general que rige los contratos, así como la que regula la contratación electrónica y los servicios de la información, es decir, el Código civil; la Ley 34/2002, del 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico; la Ley 59/2003, del 19 de diciembre, de Firma Electrónica y la Ley 21/2011, del 26 de julio, de Dinero Electrónico [\[953\]](#).

En este sentido, afirma Legerén-Molina que los contratos inteligentes –esto

es, los acuerdos que se expresan mediante código informático y no sólo éste último– son una *modalidad de los contratos electrónicos* y, por ello, suscitan problemas jurídicos similares –p. ej. la falta de contacto personal entre los contratantes, todo lo relativo a la forma y documentación del contrato o la despersonalización del consentimiento contractual–. En base a lo anterior, se aplicarán a los contratos inteligentes la normativa que regula los contratos electrónicos, con las pertinentes adaptaciones ^[954], mientras se cumplan todos los requisitos propios del concepto tradicional de los contratos, e independientemente que se trate de un negocio donde solo parte del contrato esté escrito en código –o incluso todo él–, o incluso de nuevos contratos suscritos por máquinas, pero que se concluyen de acuerdo con unos parámetros previamente establecidos.

Debe aclararse que el autor citado plantea cinco interrogantes jurídicos vinculados al *género* de los contratos inteligentes –i.e, sin poner énfasis particular en una de sus especies, los *blockchain-based Smart Contracts* ^[955]:

- i) si reúnen los requisitos esenciales de cualquier contrato de modo que puedan ser considerados como tales;
- ii) si las diferencias existentes en su proceso de formación impiden la aplicación de la normativa relativa a los contratos;
- iii) si cabe el vicio del error en ellos y cuál sería la incidencia en la responsabilidad que eventualmente se pueda derivar;
- iv) si es posible –y, en tal caso, cómo– introducir los *Smart Contracts* en el proceso; y
- v) cómo se realiza el pago en este tipo de contratos ^[956].

3.4.5.1.1. ¿Son contratos en sentido legal?

Se señala, con razón, que para que el acuerdo que incluya cláusulas “autoejecutables” sea efectivo, ha de reunir todos los requisitos tradicionalmente exigidos a los contratos, y así, se puede afirmar que –en

opinión que se comparte– la denominación de contratos inteligentes no sería más que un modo de referirse a unos contratos “tradicionales” de carácter electrónico, donde parte o todas las prestaciones están redactadas en el código y se ejecutan de manera autónoma y automática.

Los *Smart Contracts* serán, por tanto, una variedad del “contrato tradicional” caracterizado por la existencia de cláusulas autoejecutables, no siendo, entonces, necesario aplicar un régimen jurídico diverso del de los contratos, y, de manera específica, del de los electrónicos [\[957\]](#).

En consecuencia, en España, se afirma que a los contratos inteligentes le son aplicables el art. 23 de la Ley N° 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico [\[958\]](#). Avanza el autor citado analizando si los contratos inteligentes celebrados entre máquinas son, también, contratos. Para responder la cuestión, han de analizarse los elementos del contrato de acuerdo a la legislación española.

3.4.5.1.1.1. Objeto, causa y consentimiento del contrato

El Código civil español exige para que se pueda hablar de contrato que exista un objeto cierto que sea materia del contrato [\[959\]](#), sea cual fuere la prestación a que se obligan ambas partes –en este caso representadas por máquinas [\[960\]](#)–: prestación de dar, de hacer o de no hacer. Por tanto, la *existencia* de objeto confirma el carácter contractual de tales acuerdos, siempre y cuando reúna los demás requisitos: que recaiga sobre cosas posibles y que estén “dentro del comercio”, o sobre servicios que no resulten de imposible ejecución, que no sean ilícitos ni vayan contra las buenas costumbres y que el objeto sea determinado o determinable [\[961\]](#). Lo mismo cabe decir respecto de la causa de los contratos [\[962\]](#).

Respecto del consentimiento, se afirma que a la vista del carácter no humano de las computadoras y del software, sería imposible emitirlo, toda vez que el consentimiento únicamente puede ser otorgado por personas y supone la exteriorización de una voluntad interna. Sin embargo, se sostiene

que tal obstáculo se puede salvar acudiendo a la figura del precontrato y a la emisión del consentimiento de manera anticipada por las partes ^[963], subordinando, en tal caso, el contrato definitivo al cumplimiento de determinadas circunstancias. En este supuesto, si las condiciones se cumplen, el consentimiento se entiende otorgado ya en el momento de efectuar el precontrato. Cuando las partes aceptan el contenido del acuerdo y lo vuelcan en el código, están dando su consentimiento por adelantado a los futuros contratos que automáticamente se vayan a concluir –cumplidos, lógicamente, los parámetros que establezcan ^[964], y la legislación española admite la forma electrónica de consentir ^[965].

3.4.5.1.1.2. *Forma del contrato*

Afirma Legerén-Molina que en España rige el principio de libertad de formas tanto en materia civil como comercial ^[966], y la legislación admite la equivalencia de los documentos electrónicos y los escritos ^[967]. Ahora bien, los contratos formales que requieran escritura pública, no podrán celebrarse sino respetando la forma impuesta por la ley ^[968]. Asimismo, cuando un contrato inteligente tenga contacto con consumidores, deberán cumplirse los requisitos de forma y sustancia para éstos casos impuestos ^[969].

3.4.5.1.2. *Proceso de formación del contrato inteligente*

Siempre siguiendo a Legerén-Molina, afirma que dada la característica esencial de los *Smart Contracts*, –i.e. desarrollar de manera automática la consecuencia anudada si las condiciones preestablecidas se cumplen–, ello no afecta al proceso de formación del contrato, que es idéntico al de un contrato tradicional ^[970]:

Así las cosas, lo único distintivo y especial, es que ambas partes habrán condicionado la ejecución de sus prestaciones –lo que da lugar a la

consumación o fin del contrato– a un evento futuro. En consecuencia, los requisitos para la perfección del contrato contenidos en la teoría general del contrato permanecen invariados, toda vez que lo peculiar reside principalmente en el ámbito de la ejecución de la prestación ^[971].

En este sentido, el proceso de formación del contrato inteligente implicará, al igual que al celebrar un contrato tradicional, que las partes verifiquen que las exigencias legales en la formación del contrato se cumplen y que están suscribiendo un acuerdo que producirá efectos legales. Lo anterior será así tanto se trate de un contrato tradicional con parte del clausulado escrito en el código –donde una parte del contrato está informatizada–, como cuando el contrato se concluya por medio de dispositivos automáticos ^[972].

Ahora bien, también se señala que la situación será distinta cuando la consecuencia que automáticamente se ejecuta al cumplirse las condiciones preestablecidas sea, en sí, la conclusión de un nuevo contrato con todos sus elementos y no sólo la determinación de alguno de sus aspectos –ya por una de las partes, ya por un tercero–. Si la consecuencia de un contrato inteligente es justamente celebrar un nuevo contrato, propone Legerén-Molina que, a falta de una eventual regulación específica que prevea de manera concreta este tipo de negocios jurídicos, una de las categorías que mejor se puede adaptar es la del precontrato –siempre dependiendo de lo que hayan decidido y querido las partes pues pueden configurar de diversas maneras la relación jurídica– ^[973].

3.4.5.1.3. *El error en la formación de contratos inteligentes*

También analiza Legerén-Molina la incidencia del error ^[974] en la celebración de *Smart Contracts*, y afirma con razón que deberá extremarse la cautela antes de celebrar contratos inteligentes, lo que se traducirá en una elevada compenetración entre juristas y programadores para volcar adecuadamente el contenido de las cláusulas en el código, ya que las dificultades podrían derivarse de un defectuoso conocimiento de la realidad, de transmitir instrucciones comerciales incorrectas, de expresar mal las

cláusulas del contrato, o, en fin, de una deficiente programación ^[975]. Sin embargo, si a pesar de la mayor cautela, ocurre un error apto ^[976] para invalidar el consentimiento, el contrato inteligente sería anulable.

3.4.5.1.4. *La prueba del contrato en juicio*

Respecto a su prueba en juicio, se señala que puede ser necesario iniciar una acción judicial si existen deficiencias en la ejecución material que pudiesen dar lugar, por ejemplo, a una reclamación por incumplimiento, o cuando la entrega de mercancía no esté en correcto estado –por errores de fabricación, embalaje, o transporte– ^[977]. En tal evento, será necesario *traducir* el contenido del código al lenguaje usual, sin que se deba presumir el conocimiento informático por parte del tribunal a fin de interpretar y conocer el contenido contractual codificado.

Esta traducción no será problemática cuando exista una versión *tradicional* del contenido codificado de los contratos inteligentes que haya sido utilizado, por ejemplo, para que las partes emitiesen su consentimiento: sea un texto escrito en papel que las partes firman, sea una página web al que dan su consentimiento ^[978], siendo de aplicación lo dispuesto en materia de firma electrónica para contratos *firmados electrónicamente*, ya que “el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio” ^[979].

3.4.5.1.5. *El pago en los contratos inteligentes*

Finalmente, se analizan algunas cuestiones vinculadas al pago ^[980], entendido éste como la realización efectiva de la prestación pactada en el acuerdo, que sólo se entenderá cumplido cuando se ejecute de manera exacta la prestación debida, respetando los requisitos de integridad, identidad e indivisibilidad ^[981].

Con razón señala Legerén-Molina que el incumplimiento de la prestación debida no debiera ocurrir –aunque de hecho *pueda* ocurrir– al establecerse con carácter automático la ejecución de la prestación, toda vez que una nota distintiva de los contratos inteligentes no es que hagan más sencilla la ejecución, sino que la “hacen inevitable”, siempre y cuando el obligado no realice actos que obstruyan tal *autoejecución*, e.g. no mantener abierta la cuenta de que se trate y desde donde se ha de efectuar el abono previsto [\[982\]](#). Salvo por este *feature* distintivo, se le aplica al pago en los contratos inteligentes las mismas normas que a los contratos convencionales con relación al lugar del pago, al tiempo del pago, a los gastos asociados al pago, al recibo de pago, con algunas precisiones respecto al pago efectuado por un tercero, al pago al acreedor aparente, a la dación en pago y a la imputación del pago [\[983\]](#).

3.4.6. Japón [\[984\]](#)

Japón es uno de los mercados de criptomonedas más grandes del mundo, el segundo en volumen de operaciones, fue el primer país del mundo en reconocer Bitcoin como un medio legal de pagos en 2017 [\[985\]](#) y, a la vez, el primero en regular la industria de los *Exchanges* en Septiembre de 2017 [\[986\]](#), sector que a marzo de 2020 ya cuenta con 23 *Exchanges* con licencia para operar [\[987\]](#). Cuenta además con una importante asociación [\[988\]](#) que los aligutina, constituida con la finalidad de auto-regular al sector [\[989\]](#).

También desde 2017 existe en Japón un *SandBox* y el Gobierno Japonés realiza periódicamente *Hackatones en Blockchain* [\[990\]](#). En la vereda de enfrente, China hizo exactamente lo contrario, prohibiendo la creación y el trading de criptomonedas [\[991\]](#).

Ahora bien, a pesar de su gran relevancia, la legislación japonesa no tiene una definición general de activos digitales, sino que leyes especiales (la ley de

Servicios de Pago y la ley de Instrumentos Financieros y Casas de Cambio) fueron modificadas en su momento para incluir los tres tipos usuales de tokens: *payment* –llamados criptoactivos Tipo 1^[992]–, *utility* –llamados criptoactivos Tipo 2^[993]– y *security* –llamados ahora ETRs^[994]. También existe una regulación específica para las StableCoins^[995].

Por otro lado, recuérdese que en Japón también ocurrieron los tres importantes ciberataques que son, a la fecha, los robos de criptomoneda más grandes de la historia: Mt Gox^[996], CoinCheck^[997] y Zaif^[998]. Ello motivó una investigación muy exhaustiva –que se analiza *infra*–^[999], lo que, a su turno, produjo importantes cambios legislativos en 2019 en materia de criptoactivos y *Exchanges*^[1000], que entrarán en vigor en Mayo de 2020^[1001]. También se produjeron cambios en la forma en la que la Financial Services Agency (FSA) analiza los protocolos de *blockchain* y las ICOs que se pueden usar o difundir para la venta, habiendo creado una “lista blanca” y una “lista negra” de protocolos de *blockchains* y ICOs^[1002]. Debe también destacarse que Japón fue sede del primer lanzamiento de una IEO^[1003] por parte de QUOINE en 2017^[1004].

3.4.6.1. Informe del Grupo de Estudios de los Servicios de Cambio de Monedas Virtuales^[1005]

Este importante informe fue publicado en Diciembre de 2018, apenas 12 meses después del ciberataque a CoinCheck, y recomendó a la Financial Services Agency (FSA) establecer un nuevo marco regulatorio para los criptoactivos, el que fue finalmente sancionado por el Congreso Japonés en Mayo de 2019, modificando dos leyes, la que regulan los *Settlement of Funds and Financial Instruments* y la que regula a los *Exchanges* y entrará en vigor en Mayo de 2020^[1006]. Muchos han afirmado que este nuevo marco

regulatorio será probablemente una pauta de regulación seguida por otros países del mundo [\[1007\]](#).

3.4.6.1.1. Nueva definición de criptoactivos

Las modificaciones legislativas impulsadas por la FSA crean una nueva definición: la de criptoactivos, antes denominados monedas virtuales, con la declarada intención de no asociar curso legal a todas las criptomonedas [\[1008\]](#). El término criptoactivo no incluye a los security tokens, ahora denominados ETRTs [\[1009\]](#).

3.4.6.1.2. Servicio de custodia de criptoactivos

Es común que el usuario de criptoactivos no tenga consigo sus llaves privadas, sino que recurra a servicios de custodia brindados por terceros, tanto *Exchanges* como *Wallets*. La legislación japonesa define la actividad de gestión de criptoactivos [\[1010\]](#), y ahora obliga a mantener todas las llaves privadas de sus clientes en billeteras off-line, para evitar que vuelvan a suceder robos como los de Mt Gox y CoinCheck [\[1011\]](#).

3.4.6.1.3. Regulación de los Exchanges

La legislación japonesa –tanto la anterior como la que ha entrado en vigor en Mayo de 2020– considera que el ofrecimiento público de utility tokens – ICOs– es una actividad de cambio regulada, por lo cual cualquier emisor debe solicitar y obtener una licencia como *crypto asset Exchange service provider* [\[1012\]](#), o bien contratar a un *Exchange* debidamente registrado [\[1013\]](#), y en éste caso, el *Exchange* puede actuar sólo como intermediario [\[1014\]](#), o por cuenta y nombre propia, comprando y vendiendo

tokens [\[1015\]](#). Los *Exchanges* están obligados a auditar los *Smart Contracts* que se utilicen en la ICO propuesta antes de la emisión del token [\[1016\]](#). Como se dijo antes, en Japón están también regulados los IEOs, los tokens propios de los *Exchanges*. Los *Exchange* pueden también actuar como *Wallets*, pero en este caso deben cumplir ciertas condiciones adicionales [\[1017\]](#).

3.4.6.1.4. *Electronically recorded transferable rights (ERTRs)*

La reforma del año 2019 creó la figura de los ERTRs, una nueva regulación específica y agravada para un tipo especial de STOs, aquellos que tienen una tranzabilidad (i.e. liquidez) aumentada [\[1018\]](#). Se los define como un security [\[1019\]](#) token “*represented by proprietary value transferrable by means of an electronic data processing system (limited to cases where the proprietary value is recorded by an electronic device or otherwise by electronic means)*” [\[1020\]](#), que además no tienen ninguna limitación a su transmisión [\[1021\]](#).

Ahora bien, existen otros tipos de tokens digitales que no son considerados ERTRs por ser menos tranzables por no estar apalancados en tecnologías DLT [\[1022\]](#), siendo una especie de *restricted security* –usando terminología de EE.UU–.

La emisión –i.e, creación– de ERTRs está sujeta a obligaciones adicionales, tales como registrar previamente la emisión –salvo excepciones– y presentar un prospecto [\[1023\]](#), presentar cada 6 y 12 meses información económica y financiera sobre el emisor [\[1024\]](#), y obtener una licencia tanto como emisor, como para ofrecer negocios vinculados a los ERTRs [\[1025\]](#).

3.4.6.1.5. *Derivados sobre criptoactivos*

El mercado de derivados permite celebrar contratos de opción [\[1026\]](#) de compra o de venta, contratos por diferencia, y contratos de futuros sobre criptoactivos –principalmente bitcoins–, así como otros contratos más complejos como los swaps [\[1027\]](#) de manera apalancada. El mercado global de criptoderivados creció 10 veces entre 2017 y 2018 en términos de volumen operado [\[1028\]](#) y, como con mucha razón un célebre inversor dijo: los derivados son *armas financieras de destrucción masiva* y requieren un cuidadoso risk management [\[1029\]](#). Es por esto que la prestigiosa FCA inglesa ha propuesto en Julio de 2019 que se prohíba la venta de derivados a inversores minoristas no calificados [\[1030\]](#), ya que en promedio del 72% de los inversores en estos productos sufren pérdidas [\[1031\]](#).

El mercado de criptoderivados japonés es uno de los más grande del mundo, estaba desregulado y representaba el 90% de las transacciones sobre criptoactivos en 2019, es decir, el mercado de contratos en el futuro es más de 4 veces el tamaño del mercado de contratos al día [\[1032\]](#). Por tal razón, se ha sostenido que el (gran) riesgo que se corre es:

“as the derivatives market has grown exponentially, we have now entered a period where the **underlying physical exchanges are much smaller than the derivatives exchanges** – only 10% of total volumes in aggregate. It has become **tempting to try to manipulate the less liquid underlying exchanges to yield some profits trading the derivatives.**” [\[1033\]](#) (el resaltado es mío)

El mercado japonés de derivados cambiará a partir de Mayo de 2020 con la entrada en vigor del nuevo marco regulatorio, que limita el apalancamiento fuertemente a 2 veces [\[1034\]](#), cuando hasta el momento se venía operando con un apalancamiento contra el margen de garantía de 15 [\[1035\]](#) y hasta 25

veces [\[1036\]](#) .

3.4.6.1.6. *Actos desleales con criptoactivos*

La nueva regulación japonesa regula también la publicidad de servicios sobre criptoactivos, estipulando incluso penas de prisión por publicidad engañosa [\[1037\]](#) , y se penalizan ciertos actos de manipulación de mercado con penas de hasta 10 años de prisión [\[1038\]](#) .

3.4.6.2. *Informe del Ministerio de Economía, Comercio e Industria de Japón* [\[1039\]](#)

En Marzo de 2018, el Ministerio de Economía, Comercio e Industria publicó un interesante informe sobre el potencial de los *blockchain-based systems* en Japón, en el que identificó ciertas áreas con gran potencial, como salud y logística, y también abordó la cuestión de la naturaleza jurídica de los *Smart Contracts*.

En materia de salud, se divisó gran potencial en lo relativo a estudios clínicos de nuevas drogas, utilizando la *blockchain* para que los distintos *stakeholders* (empresas farmacéuticas, clínicas de prueba médica, investigadores, universidades y los denominados *contract research organizations*, CROs) puedan compartir información vinculada. En materia de logística, se auguró un uso potencial importante para la trazabilidad de baterías de autos eléctricos, llevando un registro distribuido del valor residual de las baterías, las que pueden ser reutilizadas por otras industrias, como la de generación solar, dependiendo de si tienen o no un valor residual mínimo.

Finalmente, con relación a los contratos inteligentes en la legislación japonesa, el Informe sostiene que los contratos inteligentes son legalmente válidos, pero para “*Smart Contracts that are written in machine language and are automatically executed, preliminary consensus among the relevant parties including understanding of its structure are necessary for the contract to be*

effective [\[1040\]](#).” El estudio también recomienda que, si un contrato inteligente tendrá contacto con consumidores, entonces “the contract contents for consumer interface be readable in natural language” y que “clearly state that *Smart Contract* is used and the contract details, and to get consent from the user in advance. [\[1041\]](#),”

3.4.7. Corea del Sur

El caso de Corea del Sur es también relevante, ya que actualmente es el tercer mercado de criptoactivos por volumen, luego de EE.UU y Japón [\[1042\]](#), pero llegó a ser el líder del mercado de criptoactivos en 2017, cuando un tercio de su población había invertido en criptoactivos, lo que representaba el 30% de todo el volumen de criptomonedas mundial [\[1043\]](#). Para tomar una dimensión, repárese en el hecho que existían 70 *Exchanges* en Septiembre de 2019 [\[1044\]](#). Pero esto cambió rápidamente a medida que el enfoque político comenzó a percibir (fundados) riesgos en la criptoconomía, como se verá más abajo.

Sin embargo, el Banco Central de Corea del Sur está analizando utilizar *blockchain* para llevar el registro de los bonos que se emiten, siendo el coreano uno de los mercados de bonos más grandes de Asia, con mucha actividad en bonos verdes y sociales [\[1045\]](#). El ecosistema incluiría nodos para el Banco Central, el regulador bursátil y las instituciones financieras [\[1046\]](#). Por otro lado, el Banco Central también creó en Diciembre de 2019 un grupo de trabajo para analizar la viabilidad de emitir una CBDC [\[1047\]](#). De hecho, Seúl analizó en 2018 emitir un token propio, llamado S-Coin, para acceder a servicios municipales [\[1048\]](#), y lo lanzó en 2019 [\[1049\]](#). Los vecinos de Seúl pueden ganar S-Coins participando en encuestas y pagando impuestos [\[1050\]](#).

Pero en materia de criptoactivos, desde 2017 a la fecha ha habido mucha polémica. En efecto, el Servicio de Supervisión Financiero coreano, el

regulador bursátil, amagó seguir el criterio chino y, luego de ser líderes del mercado en 2017, en 2018 se decidió prohibir –mediáticamente, sin una ley del congreso– el *trading* de criptomonedas anónimas [\[1051\]](#) en *Exchange* coreanos [\[1052\]](#) y la emisión de toda clase ICOs por parte de empresas coreanas [\[1053\]](#). Se impuso también un impuesto a las ganancias específico para todos los *Exchanges*, en una alícuota del 22% [\[1054\]](#).

Se sostuvo que “The government is concerned about manipulation of market conditions and injection of illegal funds while market funds are leaked into speculative investments” [\[1055\]](#). El gobierno coreano incluso prohibió a sus funcionarios que transaccionen en criptoactivos [\[1056\]](#), luego que salieran a la luz casos de insider trading en con criptoactivos por parte de funcionarios públicos [\[1057\]](#).

Recientemente, en Marzo de 2020, se aprobó una ley que impone estrictos controles de AML-KYC para empresas que operan criptoactivos [\[1058\]](#), obligando a los *Exchanges* y a los bancos a informar sus transacciones a la Korean Financial Intelligence Unit [\[1059\]](#). En Agosto de 2020 entrará en vigor una nueva regulación, primera en su especie a nivel mundial [\[1060\]](#), que regula las Finanzas Decentralizadas (*DeFi*), tanto los préstamos peer-to-peer con criptoactivos como también todas las plataformas de *crowdlending*, incluso con moneda fiat [\[1061\]](#). La medida se toma luego de que un estudio indicara que el 15.8% de los préstamos otorgados son incobrables, cuando en 2017 este ratio era del 5.5 y la mora ronda el 20% de la cartera [\[1062\]](#).

Finalmente, luego de más de dos años con avances, retrocesos y muchas polémicas en materia de criptoactivos, en Marzo de 2020 se aprobó por unanimidad en el Congreso coreano una legislación general sobre criptoactivos que entrará en vigor en Septiembre de 2021 [\[1063\]](#).

La norma regula a los *Exchanges* y a las *Wallets*, los obliga a obtener un certificado de seguridad informática, y se establecen penas de prisión de hasta 5 años por incumplir la nueva regulación. Además, reconoce de manera expresa a los criptoactivos como una propiedad bajo la legislación coreana. Como nota (muy) sobresaliente, se obliga a todo el ecosistema –*Exchanges, wallets*, y emisores de ICOs en general– a operar con nombre real del cliente, al obligar a abrir una cuenta bancaria en nombre de cada cliente para poder cambiar monedas fiat por criptomonedas. En adición, y como se indicó antes, existe una regulación blanda, las *Directrices sobre IEOs* preparadas por el Korea University's Cryptographic Exchange Research Institute, la Block Chain Industry Promotion Association, y la Korea *Blockchain* Startup Association [\[1064\]](#).

3.4.8. Francia

El caso de Francia también merece detenerse, ya que los franceses apiran a ser un *crypto-hub* europeo [\[1065\]](#). En un discurso dado ante la Asociación Europea de Depositarios Centrales de Títulos Valores (ECSDA, en inglés), en Noviembre de 2019 el Presidente de la Autoridad Francesa de Mercados Financieros (AMF), a la vez que alababa los rápidos cambios regulatorios de Suiza, afirmaba lo siguiente:

“Although DLT may aggravate some risks such as cyber-risks and raise new supervisory challenges, **it could also bring obvious benefits** to the post-trade environment such as faster settlement and confirmation processes and easier reporting structures. It could also aim, in the medium term, to reduce costs and speed some processes up that are too manual and too costly. **It is therefore important to encourage and facilitate its development**, starting with certain market segments where scalability is not an issue and where financial stability concerns are not significant.

The existing legal environment does not facilitate the use of

DLT and, in some cases, it even prevents experimentation. Based on analysis recently carried out by the French AMF, I note for example that the **EU legal environment regarding finality and settlement of transactions creates strong impediments** to the development of security tokens listed on trading platforms, which characterise financial instruments. Such impediments are, for example: (i) The obligation to **identify a manager** of the blockchain acting as a securities settlement system; (ii) The requirement that a credit institution or an investment firm **intermediates** the access to the securities settlement system for individuals; (iii) The fact that **ownership rights are acknowledged at custodian level** and not simply on the basis of the registration of the security tokens on a blockchain; and (iv) The **obligation to settle transactions in cash**, central bank money or commercial bank money, which is not the case on blockchains that would need a dedicated stable coin in order to settle operations. [\[1066\]](#)” (El resaltado es mío).

Así, recientemente en el Art. 26 de la llamada ley “ómnibus” *PACTE* [\[1067\]](#) se han regulado expresamente los utility tokens y los Digital Assets Services Providers (DASPs) en la llamada Ley de Crecimiento Empresarial y Transformación [\[1068\]](#), quedando bajo supervisión de la AMF, a quien deberán presentarse los White Papers y todo el material publicitario que se pretenda usar [\[1069\]](#). Pero el enfoque francés es realmente innovador, como se verá a continuación.

3.4.8.1. Registro voluntario de utility tokens. Definición de propiedad

La nueva regulación estipula [\[1070\]](#) que los *utility* tokens son una propiedad intangible, que representa en forma digital uno o más derechos que pueden emitirse, registrarse, retenerse o transferirse a través de un sistema de registro distribuido donde se identifica, directa o indirectamente,

al dueño [\[1071\]](#) .

Se aclara que el ofrecimiento público de venta de utility tokens a una cantidad limitada de personas –según lo determine la AMF– no constituye una oferta pública, y que los tokens que tengan características de instrumentos financieros, deberán cumplir además las normas atinentes a éstos [\[1072\]](#) .

Debe señalarse como muy innovador el enfoque francés, ya que los emisores podrán, *voluntariamente* solicitar un permiso –una *visa*, en términos de la ley– a la AMF para ofrecer mayores garantías a los potenciales adquirentes de tokens, lo que permite que dicho ICO se incluya, a su vez, en una lista blanca de acceso público. La AMF definirá los requisitos a cumplir para obtener el permiso y ser incluidos en la lista blanca [\[1073\]](#) . El emisor deberá constituir o registrar una persona jurídica en Francia, y establecer mecanismos de resguardo y custodia de los fondos captados y cumplir con las normas AML-KYC para poder hacer ofrecimiento público y masivo. La AMF no realiza auditoría técnica sobre los contratos inteligentes involucrados.

En Diciembre de 2019 se autorizó la primer ICO presentada voluntariamente a la AMF [\[1074\]](#) . Cuando la AMF autoriza una ICO, implica que:

“The AMF visa does not in any way constitute an assessment as to whether or not it is appropriate to participate in a token offer. It means that in the context of this public offering of tokens, **the issuer has provided the minimum guarantees required by law and that the white paper is complete and understandable** to investors. The visa does not imply either approval of the appropriateness of the issuer's project or authentication of the financial, accounting and technical information presented. Moreover, the **AMF does not carry out any verification of the Smart Contracts linked to the offering and does not verify the adequacy of these Smart Contracts with the content of the white paper**. Finally, for each offer, the

public is invited to consult the risk factors section of the information document.

This approval is optional. In other words, **ICOs without AMF approval are legal**. However, ICOs that do not have visa and unlicensed service providers will be prohibited from solicitation, patronage and sponsorship activities. [\[1075\]](#)”

3.4.8.2. *Tratamiento de los security tokens. Propuesta de SandBox europeo. Modificaciones requeridas*

En relación a los *security tokens*, la AMF considera que ciertas normas aplicables a todos los títulos valores son aplicables también a los STOs, e.g. normas sobre prospecto de emisión, pero también destaca que el marco regulatorio actual a nivel comunitario, no pensado para STOs, plantea dificultades para el desarrollo de los STOs, por lo cual la AMF impulsa a nivel Europeo un *SandBox* que permita a las autoridades nacionales relajar ciertos requisitos a cambio de determinadas garantías [\[1076\]](#).

La AMF reconoce que:

“It should be noted that **new players are emerging in this environment of "tokenised" financial instruments**. These are the "tokenisation" platforms aiming to provide a whole range of services relating to legal compliance, technical security and establishing relations between project owners and potential investors (e.g. Polymath, Harbor). This phenomenon seems to be influenced, to some extent, by the debate in the United States regarding the classification of crypto-assets. For example, an increasing proportion of the tokens issued in recent months tended to be termed "securities" by their issuers, both in anticipation of the Securities and Exchange Commission's interpretation and **to counter the decline in the popularity of ICOs**, since by using an issue of financial instruments the fundraising operation is lent a **presumption of credibility**.

[\[1077\]](#)„

3.4.8.2.1. *Casos de STOs franceses*

La AMF señala que, a Febrero de 2020, se han emitido siete STOs en Francia, ninguno de los cuales puede ser considerado un genuino ofrecimiento público, sea por los montos involucrados, como por los inversores [\[1078\]](#).

3.4.8.2.2. *Prospectos de emisión e intermediarios*

Afirma la AMF que las normas que regulan el prospecto de emisión de títulos valores convencionales se aplican también a los STOs que sean acciones o títulos de deuda, aunque reconoce la dificultad que generan muchos *security tokens híbridos*. Ahora bien, puntualiza que en los STOs es difícil definir en qué territorio la oferta tendrá lugar [\[1079\]](#) y que, al igual que para los ICOs, los emisores de STOs deberán cumplir normas de AML si no utilizan intermediarios debidamente registrados en la AMF.

3.4.8.2.3. *Know Your Customer/Client. Restricciones a la transferencia*

En relación a la anonimidad en *blockchain*, la AMF sostiene que es esencial en los STOs conocer la identidad del adquirente, especialmente cuando la emisión tokeniza participaciones sociales. A su vez, las restricciones a la transferencia deben ser programadas en el *Smart Contract*.

3.4.8.2.4. *Plataformas de trading de STOs*

Es aquí donde la AMF aprecia las mayores dificultades regulatorias, a nivel comunitario, a punto tal de afirmar que no existe ninguna a nivel europeo a

Febrero de 2020^[1080], ya que le son aplicables las regulaciones de la Directiva Europea sobre Mercados de Instrumentos Financieros y Servicios de Inversión (en inglés, MiFID I y MiFID II)^[1081], que, entre otras cosas, obliga a identificar a un responsable de la plataforma, lo que es difícil en casos de redes descentralizadas como *blockchain*^[1082].

3.4.8.3. Registro voluntario de DASPs. Registro obligatorio

Finalmente, La ley *PACTE* regula también a varios proveedores de servicios de activos digitales, término que incluye a las ICOs y también a las criptomonedas. Las categorías de servicios que quedan cubiertas son: *wallets*, *exchanges*, plataformas de *trading* de criptoactivos, gestión de patrimonios de criptoactivos, asesoramiento en inversiones en criptoactivos, y también la pre-suscripción de criptoactivos^[1083].

Muy innovadoramente, se dispone que *casi* todos los proveedores de servicios vinculados a activos digitales podrán, *voluntariamente*, solicitar un permiso a la AMF, para formar parte de una lista blanca específica para segmento de servicios con licencia. Para ello deberán cumplir requisitos relacionados a riesgo de fraude, riesgos operacionales, mecanismo de control interno y seguridad informática, y normas de prevención de conflictos de intereses, así como a la publicidad de sus servicios e información pública sobre sus comisiones y aranceles^[1084]. Si no solicitan la licencia a la AMF, ello no implica que se presuma la ilegalidad de su accionar^[1085], pero deberán igualmente cumplir las normas aplicables en materia de AML/KYC.

Ahora bien, será obligatorio registrarse en la AMF si quieren ofrecerse servicios de custodia o cambio de criptomonedas contra monedas fiat^[1086], analizándose la reputación y competencia de sus directivos y la existencia de mecanismos de AML/KYC.

Finalmente, la AMF publicará listas negras de ICOs y DASPs que no cumplan con la regulación.

3.4.9. México

El 9 de Marzo de 2018 se publicó en el Diario Oficial de la Federación el decreto que puso en vigor la llamada *Ley Fintech* de México [\[1087\]](#). En sus arts. 4 y 30, respectivamente, la ley definió los *activos virtuales* y a las *Instituciones de Tecnología Financiera* (ITFs):

“ITF: instituciones de tecnología financiera reguladas en esta Ley, las cuales son las instituciones de financiamiento colectivo y las instituciones de fondos de pago electrónico”

“se considera activo virtual la **representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos**. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas. **Las ITF solo podrán operar con los activos virtuales que sean determinados por el Banco de México mediante disposiciones de carácter general**. En dichas disposiciones, el Banco de México podrá establecer plazos, términos y **condiciones que deberán observar las ITF para los casos en que los activos virtuales que este haya determinado se transformen en otros tipos o modifiquen sus características**. Para realizar operaciones con los activos virtuales a que se refiere el párrafo anterior, las ITF **deberán contar con la previa autorización del Banco de México**. El Banco de México para la determinación de los activos virtuales tomará en cuenta, entre otros aspectos, el uso que el público dé a las unidades digitales como medio de cambio y almacenamiento de valor así como, en su caso, unidad de cuenta; el tratamiento que otras jurisdicciones les den a unidades digitales particulares como activos virtuales, así

como los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades.” (los resaltados son míos).

3.4.9.1. Activos virtuales, Exchanges y Wallets

El poder de policía sobre los activos virtuales en Méjico está dado al Banco de Méjico, en estos términos conforme al Art. 32 y 33:

“Art. 32. **El Banco de México definirá** las características de los activos virtuales a que se refiere este Capítulo, así como **las condiciones y restricciones de las Operaciones y demás actos que se pueden realizar con dichos activos**, mediante disposiciones de carácter general que para tal efecto emita. Asimismo, el Banco de México establecerá **las medidas a las que deberán sujetarse las ITF para la custodia y control** que sobre los activos virtuales ejerzan al realizar tales Operaciones y actos. Para efectos de este Capítulo, se entenderá por custodia y control de activos virtuales a la **posesión de las firmas, claves o autorizaciones que sean suficientes para ejecutar las Operaciones** a que se refiere esta Ley.”

Art. 33.- Las ITF tendrán prohibido vender, ceder o transferir su propiedad, dar en préstamo o garantía o afectar el uso, goce o disfrute de los activos virtuales que custodien y controlen por cuenta de sus Clientes, excepto cuando se trate de la venta, transferencia o asignación de dichos activos por orden de sus Clientes. Las ITF solo podrán participar en la operación, diseño o **comercialización de instrumentos financieros derivados que tengan activos virtuales como subyacente, en los casos, condiciones y sujeto a los requisitos y autorizaciones que establezca el Banco de México** en disposiciones de carácter general.” (los resaltados son míos).

3.4.9.2. Información al usuario de activos virtuales

La Ley *Fintech* dispone también ciertas obligaciones de información a favor del usuario de activos virtuales:

“Art. 34.- Las ITF que operen con activos virtuales deberán divulgar a sus Clientes, además de lo previsto en esta Ley, **los riesgos que existen por celebrar operaciones con dichos activos**, lo que deberá incluir, como mínimo, informarles de manera sencilla y clara en su página de internet o medio que utilice para prestar su servicio, lo siguiente:

- I. El activo virtual no es moneda de curso legal y no está respaldado por el Gobierno Federal, ni por el Banco de México;
- II. La **imposibilidad de revertir** las operaciones una vez ejecutadas, en su caso;
- III. La **volatilidad** del valor del activo virtual, y
- IV. Los **riesgos tecnológicos, cibernéticos y de fraude** inherentes a los activos virtuales.” (los resaltados son míos).

3.4.9.3. *SandBox*

Finalmente, debe resaltarse que el régimen *Fintech* mejicano creó un *SandBox* en el Título IV de la ley bajo estudio, al que denomina *De las Autorizaciones Temporales y Operación con Activos Virtuales*, y lo divide en cuatro capítulos.

3.4.9.3.1. *Modelos novedosos*

La Ley *Fintech* mejicana define a los *Modelos Novedosos* en su art. 4, apartado XVII, como “a aquel que para la prestación de servicios financieros utilice herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento en que se otorgue la autorización temporal en términos de esta Ley”.

3.4.9.3.2. *Autorizaciones temporales. Condiciones para su concesión*

En su art. 80, la ley bajo análisis dispone:

“Las personas morales constituidas de conformidad con la legislación mercantil mexicana, distintas a las ITF, a las Entidades Financieras y a otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, deberán obtener autorización para que mediante Modelos Novedosos lleven a cabo alguna actividad cuya realización requiere de una autorización, registro o concesión de conformidad con esta Ley o por otra ley financiera. Para la operación de Modelos Novedosos, **las Autoridades Financieras según su ámbito de competencia, de manera discrecional, previa revisión del cumplimiento de los criterios y condiciones que se establecen en el art. 82 de esta Ley, podrán otorgar o negar, con la debida fundamentación y motivación, una autorización temporal condicionada** a las sociedades interesadas en prestar servicios financieros a través de estos Modelos. Dicha autorización deberá tener una duración acorde a los servicios que se pretenden prestar y no podrá ser mayor a dos años. Tratándose de las Comisiones Supervisoras, se requerirá previo acuerdo de la Junta de Gobierno respectiva para el otorgamiento de las autorizaciones a que se refiere este artículo. En caso de tratarse de actividades cuya autorización, registro o concesión competa otorgar a la Secretaría o al Banco de México, las autorizaciones temporales serán expedidas considerando los actos administrativos previstos en las leyes que regulan dichas actividades para su autorización, registro o concesión. En caso de que corresponda a la Secretaría otorgar las autorizaciones mencionadas, las Comisiones Supervisoras serán competentes para supervisar las actividades de las sociedades autorizadas para operar con Modelos Novedosos que realicen las mismas actividades reservadas a las Entidades Financieras o sujetos supervisados por dichas Comisiones Supervisoras. La

sociedad correspondiente deberá llevar a cabo las acciones necesarias para obtener la autorización, registro o concesión definitivos durante el plazo de la autorización temporal, conforme a las leyes financieras que regulen dichos actos. Cuando no realice dichas acciones, deberá llevar a cabo el procedimiento de salida a que se refiere la fracción X del art. 83 de esta Ley. En caso de que la sociedad autorizada esté realizando las acciones necesarias para obtener la autorización, registro o concesión definitivos conforme a las leyes financieras que regulen dichos actos, la Autoridad Financiera competente, a su discreción, podrá prorrogar la autorización temporal hasta por un año más, plazo durante el cual se deberán realizar todas las acciones necesarias para obtener dicha autorización, registro o concesión definitivos e iniciar las operaciones correspondientes. En la autorización que se otorgue conforme a este artículo, las Autoridades Financieras establecerán, en función del Modelo Novedoso correspondiente, **las excepciones y condicionantes al cumplimiento de los requisitos y obligaciones establecidos en las leyes financieras respectivas, así como los términos y condiciones para la prestación de los servicios de que se trate.** En el caso de las prórrogas, dichas excepciones, condicionantes, términos y condiciones podrán ser revisados a fin de que continúe la viabilidad de la sociedad autorizada para operar con Modelos Novedosos.” (Los resaltados son míos).

El art. 82 dispone las condiciones para concesión de autorizaciones temporales:

“Para el otorgamiento de la autorización temporal a que se refiere el artículo 80 de esta Ley, las Autoridades Financieras evaluarán, entre otros aspectos, el cumplimiento de los criterios y condiciones siguientes:

- I. Que la propuesta sea un Modelo Novedoso;
- II. **El producto a ofrecerse o el servicio a prestarse al público**

debe requerir probarse en un medio controlado, en términos de este Capítulo;

III. La forma en que se pretenda desarrollar la actividad reservada debe representar un beneficio al Cliente del producto o servicio de que se trate con respecto a lo existente en el mercado;

IV. **El proyecto se debe encontrar en una etapa en la que el inicio de operaciones pueda ser inmediato;**

V. **El proyecto debe poder ser probado con un número limitado de Clientes**, y

VI. Los demás que, en su caso, determinen las Autoridades Financieras competentes mediante disposiciones de carácter general.” (el resaltado es mío)

A su vez, conforme a lo previsto en el art. 83, en la solicitud de una autorización temporal, los interesados deberán:

“I. El proyecto de estatutos sociales, el cual deberá contemplar lo siguiente:

a) La realización de forma habitual o profesional, en su objeto social, de las actividades que pretenda llevar a cabo, y

b) Establecer su domicilio social en territorio nacional;

II. **La descripción del Modelo Novedoso**, la totalidad de las operaciones o actividades que pretenda realizar a través de este Modelo y el detalle de cada una de ellas, justificando la necesidad de operar con dicho Modelo Novedoso;

III. **Las políticas de análisis de riesgo, incluyendo aquellas políticas a seguir en materia de seguridad en la Infraestructura Tecnológica y de seguridad de la información;**

IV. **Las disposiciones jurídicas que regulan la actividad reservada que consideran que obstaculizan** el desarrollo de los productos o servicios a través del Modelo Novedoso;

V. Los beneficios potenciales para los Clientes del servicio o producto de que se trate con respecto a lo existente en el

mercado;

VI. El mercado objetivo o número máximo de Clientes a los que se les ofrecería el producto o servicio de que se trate, especificando en su caso, la ubicación geográfica respectiva y **el monto máximo de recursos que podrán recibir de cada Cliente, así como el monto máximo total que podrán recibir durante la vigencia de su autorización temporal;**

VII. **La forma en que habrán de resarcir los daños y perjuicios** que, en su caso, genere a sus Clientes por la prestación de los servicios que otorgue durante el periodo en desarrollo, lo cual deberá pactarse en los contratos que para tal efecto celebren;

VIII. La forma en que pretende informar y recabar el consentimiento de sus Clientes respecto a que celebrarán operaciones con sociedades autorizadas para operar con Modelos Novedosos, así como los riesgos a que se encuentran sujetos por ello;

IX. La forma, método y plazos en que habrán de cumplir con los requisitos para obtener la autorización, registro o concesión definitivos conforme a las leyes financieras que regulan el servicio a prestar;

X. **El procedimiento de salida a llevar a cabo en caso de que las Autoridades Financieras no le otorguen la autorización, registro o concesión definitivos** o concluya la vigencia de la autorización temporal o de su prórroga, según corresponda, y

XI. La demás documentación e información que las Autoridades Financieras competentes requieran al efecto.

La presentación de la solicitud de autorización a que se refiere este Capítulo deberá ser aprobada por el órgano de administración de la sociedad que pretenda ser autorizada.

Cada Autoridad Financiera deberá publicar las autorizaciones temporales que otorgue conforme a este Capítulo en un registro que será público, por lo que le darán difusión en su página de internet y contendrá anotaciones respecto de cada sociedad autorizada para operar un Modelo Novedoso, que podrán incluir,

entre otras, la revocación de la autorización. Cada Autoridad Financiera podrá establecer, mediante disposiciones de carácter general, las bases de la organización y funcionamiento de este registro, así como las anotaciones adicionales que deberá incorporar.” (los resaltados son míos).

3.4.9.3.3. Operaciones de entidades financieras con activos virtuales

La ley en cuestión regula en sus Art. 86 y 88 también los requisitos que las entidades financieras deberá cumplir si desean operar activos virtuales:

“Art. 86. Las Autoridades Financieras podrán autorizar discrecionalmente, con la debida fundamentación y motivación, a las Entidades Financieras, ITF o demás personas sujetas a su supervisión, llevar a cabo temporalmente operaciones o actividades de su objeto social a través de Modelos Novedosos cuando en su realización se requiera de excepciones o condicionantes a lo contenido en las disposiciones de carácter general aplicables, emitidas por las propias Autoridades.

Las autorizaciones temporales a que se refiere este artículo deberán ser otorgadas previo acuerdo de la Junta de Gobierno de las respectivas Comisiones Supervisoras. En caso de actividades reguladas por disposiciones de carácter general emitidas por la Secretaría o el Banco de México, las autorizaciones temporales serán otorgadas por dichas Autoridades.

En la autorización temporal que se otorgue, la Autoridad Financiera que deba resolver establecerá las excepciones, condicionantes, términos y condiciones para los productos a ofrecer o la prestación de los servicios de que se trate.

Art. 88. Las autorizaciones temporales no podrán tener una vigencia mayor a un año, prorrogable por única vez por otro año más.”

“Las instituciones de crédito podrán, con la previa autorización del Banco de México, realizar operaciones con los activos virtuales que sean determinados por el propio Banco de México mediante disposiciones de carácter general, de entre aquellos que cumplan las características mencionadas en el último párrafo del artículo 30 de esta Ley. Dichas operaciones estarán sujetas en cuanto a sus condiciones y restricciones, a las disposiciones de carácter general que para tal efecto emita el Banco de México.” (los resaltados son míos)

3.4.9.3.4. Obligaciones por la concesión de autorizaciones temporales

Concedida una autorización temporal, señala el art. 89 que los autorizados deberán presentar un reporte periódico y un informe final, donde constará:

- I. El número de operaciones realizadas durante el periodo reportado;
- II. El número de Clientes o usuarios con los que cuentan a la fecha del reporte;
- III. Las situaciones de riesgo que se hayan presentado, y
- IV. La demás información que las Autoridades Financieras requieran para tal efecto conforme a las disposiciones de carácter general que éstas emitan.

Además, las sociedades autorizadas para operar con Modelos Novedosos, ITF, Entidades Financieras y demás personas sujetas a la supervisión de las Autoridades Financieras que obtengan la autorización temporal a que se refiere este Título, **deberán entregar a dichas Autoridades Financieras un reporte final a más tardar treinta días posteriores al término de la vigencia de la autorización temporal**, en el que se describan las cifras totales respecto de la información prevista en las fracciones anteriores, así como cualquier otra que las Autoridades Financieras determinen en la autorización temporal o en disposiciones de carácter general que para tal

efecto emitan.” (los resaltados son míos).

3.4.10 Chile

La irrupción de los criptoactivos en Chile ha sido fenomenal, poniendo en valor el alto nivel institucional que Chile ha sabido construir a lo largo de los años. En efecto, Chile tiene quizás el primer pronunciamiento judicial cautelar en toda Latinoamérica referido –aunque sea indirectamente– a los criptoactivos, de la mano de su prestigioso tribunal antitrust.

3.4.10.1. El Tribunal de Defensa de la Libre Competencia y los criptoactivos

En Abril de 2018, se inició una batalla entre el sector bancario y los dos principales *Exchange* chilenos, cuando dos bancos privados decidieron cerrar las cuentas corrientes de los *Exchanges* [\[1088\]](#), imposibilitando *de facto* su operación.

Los *Exchange* afectados recurrieron al Tribunal de Defensa de la Libre Competencia (TDLC) pidiendo sendas medidas cautelares para que se obligue a los bancos a que reabran sus cuentas corrientes, y acusando a los diez bancos privados chilenos de un abuso de posición dominante colectiva, además de solicitar multas por 180 millones de Dólares. Las medidas cautelares fueron despachadas favorablemente por el TDLC [\[1089\]](#), reconociendo *a priori* el *fumus bonis iuris* invocado por los *Exchange*, lo que generó la fuerte reacción del Banco Central de Chile [\[1090\]](#) y de la Corte Suprema de Chile. Sin embargo, con un claro mensaje pro-competencia e innovación, el TDLC ha mantenido las cautelares [\[1091\]](#) que obligan a los bancos a mantener abiertas las cuentas corrientes de los *Exchange* que operan en Chile [\[1092\]](#). Un solo comentario agregaré: aplausos, más aplausos, y de pie.

3.4.10.2. La posición de la Corte Suprema de Justicia de Chile

La disputa entre *Exchanges* y Bancos chilenos llegó a la Corte Suprema de Justicia de Chile, en la causa “*ORIONX SPA C/BANCO ESTADO DE CHILE* [\[1093\]](#)”, donde la Corte se pronunció a favor de los bancos en éstos términos:

“Que de esta manera, la decisión recurrida (i.e. cerrar cuenta corriente bancaria operada por un Exchange), además de no ser ilegal tampoco es arbitraria, por cuanto se encuentra fundada en una determinación previa y de carácter general adoptada por la institución en orden a **no operar con empresas que se dediquen a la emisión o creación, corretaje, intermediación o sirvan de plataforma a las llamadas criptomonedas u otro tipo de empresas de esta naturaleza, mientras no exista un reconocimiento regulatorio de la actividad**; esto a fin de dar cumplimiento a la normativa legal y a aquella emanada de la entidad encargada por ley de fiscalizarla, que busca evitar que el banco y sus productos puedan ser instrumentalizados con la finalidad de llevar a cabo **operaciones de lavado de activos o financiamiento del terrorismo, entre otras posibles actividades riesgosas** (...) el giro de la actora comprende la compra y venta sobre monedas virtuales y criptodivisas tales como Ethereum, Ripple, Litecoin y Bitcoin, todas consistentes – según se señala en el propio recurso- en programas computacionales, específicamente algoritmos que, como tales, carecen de manifestaciones físicas y no tienen valor intrínseco como tampoco –generalmente- uno que cuente con respaldo de algún gobierno en particular o de alguna compañía, siendo definidas y controladas por un grupo descentralizado de usuarios que utilizan el protocolo de Bitcoin en internet, a lo que se suma que actualmente las actividades financieras que se realizan con ellas efectivamente carecen de marco regulatorio. Estas características y elementos determinan, por ende, **la imposibilidad actual para el Banco recurrido de cumplir las**

obligaciones ya referidas, pues obstan a que pueda conocer a fondo las actividades financieras relativas a criptomonedas que desarrolla la recurrente, las características más relevantes de sus operaciones, los fundamentos en que éstas se apoyan y, por último, si sus montos son desmedidos o no. Y es precisamente esta imposibilidad de conocimiento y de cumplir con los deberes que pesan sobre el banco lo que **da sustento a la decisión de cierre de la cuenta bancaria de la actora**, que en consecuencia no puede ser tildada de arbitraria.” (los resaltados son míos)

3.5. *Criptoactivos & Smart Contracts vs. Derecho Nacional: Lege Data y Lege Ferenda*

Habiendo analizado las principales posturas mundiales y la recepción en los ordenamientos jurídicos más relevantes de los denominados criptoactivos, sus especies, y de los contratos inteligentes, corresponde ahora analizar cuál es (o debiera ser) el tratamiento que la legislación argentina dispensa a estos nuevos fenómenos.

En un muy buen artículo, Cosola y Schmidt ^[1094] señalan la debida distinción entre, por un lado, el género de los criptoactivos digitales – llamados usualmente *digital tokens*–, y las criptomonedas en particular e.g. bitcoin y las demás monedas virtuales, e.g. ICOs. En opinión del autor, existe una relación de género a especie entre los tokens como género, y las criptomonedas como una especie dentro del género más amplio de los criptoactivos. Recientemente se ha sostenido ^[1095] que el término criptoactivo se refiere a una gran variedad de activos, no hay una única definición consensuada, y a veces el término es empleado como sinónimo con otros términos, tales como monedas virtuales, monedas, monedas digitales, y activos digitales. Así, se ha definido a los criptoactivos en general:

“as a private digital asset that: a) is recorded on some form of a digital distributed ledger secured with cryptography, b) is

neither issued nor guaranteed by a central bank or public authority, and c) can be used as a means of **exchange** and/or for **investment** purposes and/or to **access** a good or service ^[1096]”(resáltese su triple función: forma de intercambio, forma de inversión, y forma de acceso).

Ahora bien, dentro del género de criptoactivos, o *tokens*, Cosola y Schmidt precisan que:

“La palabra token tiene varios significados, dependiendo del campo de acción del cual estemos hablando. En **programación** informática, es un elemento del lenguaje de programación. En el campo de la **seguridad informática**, es un dispositivo físico electrónico que permite almacenar claves criptográficas como la firma digital o datos bio- métricos como la huella dactilar. También dentro del mismo campo, un token es una aplicación móvil (token de los bancos) que permite realizar operaciones de manera segura con una entidad determinada. En el campo de las **finanzas**, se entiende por token la representación digital de cualquier bien que pueda estar en el comercio. Token es un nuevo término para una unidad de valor emitida por una entidad privada. De la misma forma que existen las criptomonedas, existen las acciones virtuales de una empresa. A esas acciones virtuales las denominamos token. El token es una nueva herramienta de inversión a través de la blockchain. **Puede tener funciones de medio de pago, pero además puede ser la representación de una acción o de los títulos valores, un producto, una casa, puntos en la tarjeta o en un comercio, kilogramos de soja, kilovatios de electricidad, etc.** Permite que todo pueda ser comercializable. Al token se lo podría asimilar a una ficha de casino o de videojuegos. Cuando vamos al casino o a una sala de videojuegos, no podemos jugar con dinero sino con fichas que representen dinero. En este caso, a las fichas del mundo físico las denominamos token en el mundo

digital. A diferencia de las criptomonedas, cuya creación y generación no están reguladas por ninguna empresa o entidad sino que la descentralización es una de sus cualidades esenciales, los token **son generados por empresas en una blockchain** ya existente que admite contratos inteligentes (Smart Contracts). Cada empresa o cada proyecto criptográfico que realiza su ICO, crea su propio token como parte del proyecto. Quienes invierten en ellos lo hacen pensando que en el futuro el valor de esos token va a aumentar en base a la potencialidad del proyecto emprendido.” (los resaltados son míos)

Y con relación a las criptomonedas en particular, que fueron, en efecto, la primera especie de cryptoactivo en emerger en 2008/9 con Bitcoin, afirman los autores citados que:

“La criptomoneda es toda aquella **moneda creada mediante un sistema criptográfico** que utiliza su propia cadena de bloques y que sirve como medio de pago general, incluso en el mundo físico. No tiene un emisor concreto sino que su emisión y seguridad se basa esencialmente en un tipo de escritura enigmática con claves especiales que la vuelven secreta (criptografía). Las criptomonedas son una **especie de dinero digital** que tiene la capacidad de interactuar como medio de pago tanto en el mundo físico o analógico como en el mundo digital; por ello, decimos que, en consecuencia, **toda criptomoneda es también dinero digital y electrónico**. Se entiende por **monedas virtuales** todas aquellas que para su creación no necesitan necesariamente una cadena de bloques y solo tienen la **capacidad de interactuar en el mundo digital para adquirir bienes virtuales**, normalmente circunscriptos a un determinado espacio digital. Son creadas por empresas y poseen un emisor determinado. Un ejemplo de moneda virtual serían las monedas de los juegos o videojuegos donde se puede tener dinero pero para comprar los bienes en dicho juego o

ámbito circunscripto. En consecuencia, toda moneda virtual es dinero digital. [\[1097\]](#)” (los resaltados son míos)

Muchas veces, la literatura se refiere a las criptomonedas como *payment tokens*, y ello es correcto en alguna medida, ya que se refiere a un token con una funcionalidad específica: funcionar como un medio de pago o intercambio, y a la vez ser una unidad de cuenta y una reserva de valor, de manera alternativa a las monedas de curso legal emitidas por los gobiernos [\[1098\]](#). Pero como se ha visto, los *payment tokens* no son la única clase de tokens, pero sí fueron la primera especie en surgir.

Ahora bien, como también ya se ha comentado antes, los tokens i.e. activos digitales o criptoactivos, cualquiera sea su especie, pueden ser transaccionados por contratos inteligentes. La pregunta que aflora, entonces, es la siguiente ¿deben aplicárseles a los *Cryptoassets* y *Smart Contracts* las normas argentinas que rigen los derechos reales y personales, contenidas en los Libros IV y Libro III del Código Civil y Comercial de la Nación (CCCN)? ¿Deben dichas normas ser modificadas o adaptadas a los nuevos fenómenos?

3.5.1. *Criptoactivos, Contratos Inteligentes y Código Civil y Comercial de la Nación (CCCN)*

Con relación a una especie de los criptoactivos, esto es, las criptomonedas en general y bitcoin en particular –i.e. *payment tokens*–, Santiago Mora ha sostenido que su naturaleza jurídica podría ser la de un *documento digital con firma electrónica* –confr. Arts. 5 y 6, Ley N° 25.065 de Firma Digital–, o, en su defecto, un *bien* que no es una cosa, en los términos de los Arts. 15, 16 y 764 del CCCN [\[1099\]](#).

La primera definición de los *payment tokens* en Argentina fue la dada por la Unidad de Información Financiera (UIF), en la Resolución 300/2014, cuyos considerandos decían:

“Que las **monedas virtuales representan un negocio en**

expansión en el mundo entero, que ha cobrado relevancia económica en los últimos tiempos. Que, sin perjuicio de lo indicado, las monedas **virtuales involucran una serie de riesgos para el sistema de prevención de los delitos de Lavado de Activos y de la Financiación del Terrorismo**. Que el GRUPO DE ACCION FINANCIERA INTERNACIONAL, ha emitido en enero y junio del corriente año documentos relativos a los referidos riesgos que implican las mencionadas monedas virtuales, siendo uno de los más significativos el **anonimato**, lo que **impide la trazabilidad nominativa de las operaciones**. Que, adicionalmente, las monedas virtuales son muchas veces comercializadas mediante transacciones a distancia realizadas a través de internet; permiten el movimiento transfronterizo de activos, involucrando a entidades de diferentes países, **pudiendo participar de las mismas jurisdicciones que no tienen controles de prevención** de Lavado de Activos y de la Financiación del Terrorismo adecuados; todo lo cual dificulta a los Sujetos Obligados la detección operaciones sospechosas. Que estas vulnerabilidades podrían estar siendo aprovechadas por personas que pretenden evitar el sistema preventivo establecido por nuestro país mediante la sanción de la Ley N° 25.246 y sus modificatorias. Que las medidas que por la presente se implementan permitirán mitigar adecuadamente los riesgos de Lavado de Activos y de Financiación del Terrorismo en nuestro país. Que las citadas acciones encuentran correlato también con lo dispuesto en la Recomendación 1 de las 40 Recomendaciones para prevenir los delitos de Lavado de Activos y de Financiación del Terrorismo del GRUPO DE ACCION FINANCIERA INTERNACIONAL” (Los resaltados son míos).

La UIF, en el Art. 2 de la citada Resol. 300/2014, definió a las “Monedas Virtuales” como “la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún

país o jurisdicción. En este sentido **las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias**, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción.”

Tomando la definición de la UIF, la pregunta que cabe hacerse es la siguiente: ¿Pueden considerarse las monedas virtuales –i.e., *payment tokens*– como “*moneda sin curso legal que sea usada habitualmente en el tráfico*”?

[1100]

O puesto en otros términos, una obligación pactada en una criptomoneda: ¿es una obligación de valor, cuyo objeto es un bien susceptible de apreciación económica que, por sus cualidades especiales, satisface el interés del acreedor?

Si el CCCN admite expresamente obligarse en un *cierto valor*, incluso en una moneda *sin* curso legal pero con uso habitual en el tráfico, ¿Por qué no sería válido pactar un valor en una criptomoneda como bitcoins, o Ether, o en alguna criptomoneda estable, como DAIs [1101]? Máxime cuando los usos, prácticas y costumbres son vinculantes cuando las leyes o *los interesados* se refieren a ellos, o en situaciones no regladas legalmente, siempre que no sean contrarios a derecho, confr. art. 1, CCCN [1102]. Ello no es óbice para que, el deudor de *tal* valor, al momento de la cancelación pueda abonar en moneda de curso legal, al valor del día de pago de la criptomoneda utilizada, en tanto no se haya renunciado tal facultad, confr. Art. 765, CCCN [1103].

3.5.1.1. Los criptoactivos como documento digital con firma electrónica

Mora sostiene que las anotaciones en una *blockchain* cumplen con el concepto de documento digital con firma electrónica, de conformidad con los Arts. 5 y 6 de la Ley de Firma Digital N° 25.506:

“Art. 5° — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o

asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Art. 6° — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, **con independencia del soporte utilizado** para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.” (el resaltado es mío).

Indica con acierto y precisión Mora que el documento será digital en tanto y en cuanto represente digitalmente actos o hechos, sin importar el soporte, i.e. la tecnología subyacente, en el que el documento digital está almacenado [\[1104\]](#), lo que va en línea con el principio de libertad de formas consagrado en los art. 284 y 1015 CCCN:

“Art. 1015.- Libertad de formas. Solo son formales los contratos a los cuales la ley les impone una forma determinada.

Art. 284.- Libertad de formas. Si la ley no designa una forma determinada para la exteriorización de la voluntad, las partes pueden utilizar la que estimen conveniente. Las partes pueden convenir una forma más exigente que la impuesta por la ley.”

Por otra parte, indica Mora que la firma electrónica está definida de manera residual, como todo documento digital generado o vinculado a una clave que no cumpla con los requisitos de la firma digital de acuerdo al art. 2 de de la Ley de Firma Digital N° 25.506:

“Art. 2° — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de

verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.”

Concluye Mora afirmando que:

“si bien la blockchain utiliza el mismo sistema de criptografía asimétrica de clave pública que se utiliza para firmar digitalmente en Argentina, dichas técnicas no llegan a ser totalmente equivalentes en la actualidad **porque para firmar digitalmente hace falta la intervención de certificadores licenciados que en la blockchain en principio no intervienen.** Por lo anterior entendemos que en la blockchain habría en rigor firmas electrónicas. [\[1105\]](#)” (El resaltado es mío).

3.5.1.2. Los criptoactivos como un bien

También se ha sostenido que los criptoactivos son, en general, un bien, criterio que siguen los ingleses [\[1106\]](#), los norteamericanos [\[1107\]](#) y también los franceses [\[1108\]](#).

La definición de las características de las cosas y los bienes –objeto de los derechos reales–, amerita detenerse en el estudio de uno de los elementos de las relaciones jurídico-reales, entendidas éstas como la expresión de un conjunto de temáticas económicas, sociales y políticas esenciales para la organización de la vida en comunidad [\[1109\]](#).

3.5.1.2.1. Definición de bien para el derecho argentino

Los derechos reales tienen por objeto la totalidad o una parte material de la *cosa* que constituye su objeto, por el todo o por una parte indivisa, y también puede consistir en un *bien* taxativamente señalado por la ley [\[1110\]](#).

La relación existente entre bienes y cosas, se sabe, es de género a especie [\[1111\]](#), por tanto, el género *bien* incluye tanto las especies de (i) bienes materiales –llamados *cosas*–, entre las que discutiblemente se incluye a la energía y las fuerzas naturales [\[1112\]](#), y también la especie de (ii) bienes inmateriales, donde se incluyen, por ejemplo, los derechos [\[1113\]](#), las partes de interés de las sociedades de personas [\[1114\]](#), los derechos beneficiarios en un fideicomiso [\[1115\]](#); las acciones de la sociedad anónima [\[1116\]](#), las cuotas de la sociedad de responsabilidad limitada [\[1117\]](#), universalidades de derecho como la herencia [\[1118\]](#), los derechos de incidencia colectiva, los derechos sobre el cuerpo humano y de las comunidades indígenas [\[1119\]](#).

3.5.1.2.2. *El objeto de los derechos reales*

El objeto de los derechos reales, bajo la legislación argentina actual, puede comprender tanto a las cosas como a los bienes. Pero no fue siempre así.

Se ha señalado que el pensamiento clásico reinante al momento del Código Civil de Vélez Sársfield entendía que el objeto de los derechos reales eran sólo las cosas, objetos materiales susceptibles de tener valor económico [\[1120\]](#). Si bien Vélez Sársfield reguló y reconoció los derechos reales de usufructo y prenda de y sobre créditos, lo cierto es que el crédito, en tal concepción, no era *per se* el objeto del derecho real, sino que el *instrumento* donde constaba el crédito era el objeto del usufructo y la prenda de créditos [\[1121\]](#): “el instrumento cartular es una cosa como papel, pero es difícil admitir que se convierta en un inmueble por representación; el sistema de Vélez se queda con la ficción, pero es contraproducente, por disvalioso, prescindir de la

realidad”^[1122].

El Proyecto de 1998^[1123] procuró sincerar el objeto de los derechos reales, habida cuenta los innegables cambios sociales, económicos y tecnológicos registrados desde 1871. Así, incluyó expresamente a los derechos como objeto posible de los derechos reales, además de las cosas, y reguló la prenda de créditos, en la cual era el crédito el objeto de la prenda. Regulaba también como derecho real cuyo objeto es un derecho: el usufructo de derechos, el usufructo de patrimonio de origen testamentario, y el derecho real de superficie^[1124]. Este criterio influyó luego en el CCCN, como se indicó más arriba, que expresamente reconoce a los bienes como objeto de los derechos reales.

Puntualmente respecto a los *bienes* como objeto posible de los derechos reales conforme al Art. 1883 CCCN, se ha sostenido que allí la alusión a *bien* es equívoca; debió hacer referencia a *derechos*, ya que el Art. 16 CCCN define a los *bienes* como el género, y a las cosas como una especie –i.e, los derechos son la otra especie del género, no el propio género. Esta equivocación fue salvada en materia de derechos reales de garantía, ya que el Art. 2188 CCCN hace referencia a “cosas y derechos que pueden constituir su objeto”^[1125].

Así, el CCCN actual reconoce derechos reales cuyo objeto son, a su vez, otros derechos (i) sean creditorios, como es el caso de las prendas de créditos, como (ii) reales, tal el caso del derecho real de garantía sobre el derecho de plantar, forestar o construir^[1126], o el usufructo de un derecho, cuando la ley lo admite, e.g. la anticresis del usufructo. A su turno, la Ley General de Sociedades N° 19.550 permite el usufructo (y la prenda) sobre acciones de la sociedad anónima y sobre cuotas de la sociedad de responsabilidad limitada. Ni las acciones ni las cuotas son cosas^[1127].

3.5.1.2.3. *Derechos reales sobre cosas registrables*

Muy vinculado a la cuestión registral –de la cual la *blockchain* es solo una modalidad nueva y digital–, el CCCN dispone en su art. 1890:

“Derechos reales sobre cosas registrables y no registrables. Los derechos reales recaen sobre cosas registrables cuando la ley requiere la inscripción de los títulos en el respectivo registro a los efectos que correspondan. Recaen sobre cosas no registrables, cuando los documentos portantes de derechos sobre su objeto no acceden a un registro a los fines de su inscripción.”

Se ha sostenido que esta clasificación de los derechos reales no atañe directamente al derecho real, sino a su objeto. Así, pueden recaer sobre objetos registrables o no, los derechos de dominio, de tiempo compartido y de usufructo [\[1128\]](#), y necesariamente recaen sobre objetos registrables los derechos reales de propiedad horizontal, de conjuntos inmobiliarios, de cementarios privados, de superficie, de habitación, de hipoteca y de anticresis. En todos los casos citados, el objeto es un inmueble, excepto en la anticresis, que también puede recaer sobre cosas muebles registrables. La prenda sin desplazamiento recae exclusivamente sobre objetos no registrables [\[1129\]](#).

Se ha criticado la clasificación expuesta, afirmándose que lo importante no es que la cosa acceda a un registro, sino qué finalidad cumple dicho registro, si declarativa para dar oponibilidad a terceros de buena fe, o constitutiva, para dar nacimiento al propio derecho real [\[1130\]](#).

Se puede considerar que en el caso de la *blockchain*, el registro descentralizado y distribuido de un criptoactivo cumpliría ambas funciones: la de crear el activo digital –i.e., registro constitutivo– y a la vez publicitar a terceros su existencia –i.e., registro declarativo–, aunque la identidad final del propietario del criptoactivo pueda no ser conocida por todos dado que la llave pública –i.e. la dirección en la *blockchain* que aloja el activo digital– no permite necesariamente conocer al poseedor de la correspondiente llave privada, y ésta es la que, en los hechos, le confiere y otorga el control –o mejor dicho, la relación de poder [\[1131\]](#)– sobre el criptoactivo de que se trate.

3.5.1.2.4. Los criptoactivos como un commodity

Es interesante traer a colación el criterio de la Commodity Futures Trading Commission de EE.UU (CFTC), principal regulador en materia de derivados y otros productos bajo la Commodity Exchange Act, que entendió que las monedas virtuales en general son un *commodity*. En un fallo de 2018 en el caso McDonnell que se analiza más abajo § 4.7.5.4, un Tribunal de Nueva York confirmó el criterio de la CFTC [\[1132\]](#).

3.5.1.2.5. *Los criptoactivos son un bien mueble incorporal registrable*

Recapitulando, los criptoactivos, en mi opinión, son un bien mueble incorporal registrable (en una DLT) [\[1133\]](#).

Desde tal perspectiva, el documento digital con firma electrónica es, *per se*, la *forma* de su representación en un registro distribuido y descentralizado *on-chain*, así como, por ejemplo, el título marcario es la forma legal de representar la existencia y titularidad de una marca en el registro creado por el art. 4 y 10 de la Ley de Marcas y Designaciones N° 22.362 [\[1134\]](#).

Entonces, si bien se puede afirmar, en general, que la *sustancia* de los criptoactivos es la de ser un bien mueble incorporal registrable *on-chain*, también debe repararse en que algunas especies de criptoactivos *podrían*, además, estar –en tanto bienes–, sujetos a distintos regímenes jurídicos aplicables a distintas especies de bienes, como por ejemplo, el régimen de los títulos valores atípicos, o el de los títulos valores típicos, o incluso el de algunas participaciones sociales como la acción en la SA y en la SAS. En éstos casos puntuales en los que la *especie* del criptoactivo accede, por su diseño y programación, a un régimen jurídico específico –e.g. security tokens–, éste régimen prevalente definirá su naturaleza jurídica.

3.5.1.3. *¿Los criptoactivos como un título valor no cartular atípico?*

El CCCN regula en su Libro Tercero, *Derechos Personales*, Título V, *Otras fuentes de las obligaciones*, Capítulo VI a los títulos valores como fuente de

obligaciones. Se trata de la primera regulación *general* en nuestra historia, ya que hasta la entrada en vigor del CCCN existían solo regulaciones particulares respecto de especies de títulos valores, e.g., warrants, carta de porte, papeles de comercio [\[1135\]](#).

Así, la regulación contenida en el CCCN oficia de parte general, ya que no se tratan de manera particularizada las especies que integran el género de los títulos valores, regulación ésta que es objeto de leyes separadas [\[1136\]](#) y respecto de las cuales la regulación *general* del CCCN es supletoria e integradora [\[1137\]](#).

En lo que aquí interesa, la regulación del CCCN define, en general, a los títulos valores [\[1138\]](#) y regula luego a las especies cartulares [\[1139\]](#) y no cartulares [\[1140\]](#); se define a éstos como aquellos títulos que no son representados en papel, i.e. títulos valores desmaterializados.

Los títulos valores desmaterializados son aquellos en los que el título valor no tiene el sustrato material como los títulos cartulares, sino que constan, gracias a medios técnicos, en registraciones informáticas o en documentos electrónicos [\[1141\]](#). Se los define como “aquellos en lo que uno o varios sujetos, a partir de una declaración expresa de voluntad, asumen una obligación incondicional e irrevocable, confiriendo a quien resulte legitimado un derecho autónomo que no se encuentra incorporado a un documento, sino que surge del instrumento de creación y queda reflejado en los registros del emisor o de quien los lleve en su nombre.” [\[1142\]](#)

En este sentido, se afirma que la desmaterialización de los títulos valores es una de las técnicas más actuales que combina el fenómeno *técnico* (medios informáticos que permiten eliminar el soporte papel, facilitando las comunicaciones y aportando medios sofisticados de información, registración y archivo) con el fenómeno *jurídico* tradicional (documentos de carácter dispositivo, literal, autónomo donde se incorpora el derecho al documento) [\[1143\]](#).

También se afirma que con la desmaterialización, se incorporan nuevos principios a la teoría de los títulos valores: la libertad de creación y la consagración de los valores sin títulos. Así, la centralidad de los títulos valores migra desde la *necesidad* y la *literalidad* del documento, hacia un asiento registral informático, técnicamente comprobable, que atestigua el nacimiento, la subsistencia, la titularidad y la transferencia del derecho ^[1144]. El fenómeno no es tan nuevo, ya que el primer paso hacia la desmaterialización de los títulos valores fueron las acciones y las obligaciones negociables escriturales, así como los títulos fiduciarios representados mediante anotaciones en cuenta, y los comprobantes de certificado globales ^[1145].

3.5.1.3.1. Libertad de creación de títulos valores: causales vs. Abstractos

En materia de títulos valores desmaterializados, rige la libertad de creación, y por expresa disposición de la ley, los títulos creados pueden ser atípicos ^[1146]. Esta libertad de creación ya había sido reconocida en el ámbito bursátil en el año 2012, en el Art. 3 de la Ley de Mercado de Capitales N° 26.831 ^[1147], aunque Aicega señala precedentes de autorización por parte de CNV de títulos valores atípicos ya en 1971 ^[1148].

Señala también Aicega que no existe país del mundo que establezca expresamente la libertad de creación de títulos valores sin disponer alguna limitación ^[1149]. En el caso argentino, la única limitación gira en torno a los títulos valores *abstractos*, i.e. aquellos en los que existe una prescindencia jurídica de la causa: pagaré, cheque y letra de cambio, que sólo pueden crearse: (i) para ser destinados a oferta pública, cumpliendo el régimen legal aplicable; o (ii) cuando los emisores son bancos, aseguradoras o fiduciarios financieros registrados en CNV.

Ahora bien, respecto de los títulos valores *causales*, la libertad de creación es total, pudiendo ser emitidos por personas humanas o jurídicas, públicas o privadas, pudiendo crearse clases, regular su forma de circulación, estipularse garantías, rescates, plazos, su conversión en otro tipo de título valor, y toda

otra regulación que involucre derechos de los titulares y de partes interesadas. Las condiciones de su emisión deben precisar sus características, sin confundirlos con las de otros títulos valores regulados, como las acciones de la sociedad anónima, el certificado de depósito, etc [\[1150\]](#).

3.5.1.3.2. *Los criptoactivos como valores negociables*

Ahora bien, se ha comentado más arriba como la creación de security y utility tokens ha sido una tendencia muy marcada en el ámbito de la *blockchain*, con dos períodos muy claros: (i) 2015-2018: muchas emisiones de ICOs en formato *utility* tokens; y (ii) 2019-2020: muchas emisiones en formato STOs, con los primeros casos de IEOs y DAICOs.

En Argentina, al igual que otros muchos países, se ha sostenido que ciertas especies de criptoactivos pueden ser considerados *valores negociables* en el marco de la Ley de Mercado de Capitales N° 26.831 [\[1151\]](#), cuya definición es suficientemente amplia:

“Valores negociables: Títulos valores emitidos tanto en forma cartular así como a todos aquellos **valores incorporados a un registro de anotaciones en cuenta** incluyendo, en particular, los valores de crédito o representativos de derechos creditorios, las acciones, las cuotapartes de fondos comunes de inversión, los títulos de deuda o certificados de participación de fideicomisos financieros o de otros vehículos de inversión colectiva y, en general, **cualquier valor o contrato de inversión** o derechos de crédito homogéneos y fungibles, emitidos o agrupados en serie y negociables en igual forma y con efectos similares a los títulos valores; que por su configuración y régimen de transmisión sean susceptibles de tráfico generalizado e impersonal en los mercados financieros. Asimismo, quedan comprendidos dentro de este concepto, los contratos de futuros, los contratos de opciones y los contratos de derivados en general que se registren conforme la

reglamentación de la Comisión Nacional de Valores, y los cheques de pago diferido, certificados de depósitos de plazo fijo admisibles, facturas de crédito, certificados de depósito y warrants, pagarés, letras de cambio, letras hipotecarias y todos aquellos títulos susceptibles de negociación secundaria en mercados.” (el resaltado es mío).

En consecuencia, se ha sostenido –con razón– que ciertos tokens, aquéllos llamados *security* tokens, a juicio de la CNV, podrían ser considerados valores negociables con oferta pública, sujetos a autorización *previa* por parte del regulador bursátil [\[1152\]](#), al igual que la utilización de ciertos criptoactivos como activo subyacente para determinar el precio de un producto financiero, o la compra o venta de criptomonedas a un precio predeterminado y en una fecha futura, podrían ser considerados un contrato *derivado* o un contrato de futuros, respectivamente [\[1153\]](#).

Es muy importante señalar que el encuadramiento de un token como valor negociable con oferta pública lo somete al régimen imperativo de la oferta pública, y que cualquier ofrecimiento en infracción a dicho régimen, habilita a la CNV a iniciar una acción penal en los términos del Art. 310 del Código Penal, que dispone:

“Art. 310.- Será reprimido con prisión de uno (1) a cuatro (4) años, **multa de dos (2) a ocho (8) veces el valor de las operaciones realizadas** e inhabilitación especial hasta seis (6) años, el que por cuenta propia o ajena, directa o indirectamente, realizare actividades de intermediación financiera, bajo cualquiera de sus modalidades, sin contar con autorización emitida por la autoridad de supervisión competente. En igual pena incurrirá **quien captare ahorros del público en el mercado de valores o prestare servicios de intermediación para la adquisición de valores negociables, cuando no contare con la correspondiente autorización emitida por la autoridad competente.**

El monto mínimo de la pena se elevará a dos (2) años cuando se hubieran utilizado **publicaciones** periodísticas, transmisiones radiales o de televisión, **internet**, proyecciones cinematográficas, colocación de afiches, letreros o carteles, programas, circulares y comunicaciones impresas o **cualquier otro procedimiento de difusión masiva.**” (el resaltado es mío)

3.5.1.3.3. *Utility y Security tokens vs. Ley de Mercado de Capitales*

Profundizando en los STOs, Mora y Bericua ^[1154] conceptualizan el fenómeno como una opción de financiamiento mediante la cual el promotor de un proyecto emite unos tokens sobre una plataforma *blockchain* preexistente y los ofrece al mercado a cambio de criptodivisas o moneda fiduciaria ^[1155].

En este sentido, precisan los autores que los STOs presentan la mayor problemática jurídica, dado que el token que se emite puede llegar a tener la consideración de título valor o valor negociable cuya oferta pública está sometida a regulación ^[1156]. Para definir la naturaleza jurídica del criptoactivo que será creado, debe analizarse, en primer término, la legislación sobre títulos valores de la jurisdicción del lugar donde se ha constituido el vehículo que realizará la emisión, y también en los lugares en los que la emisión pretende captar fondos ^[1157].

Afirman los autores citados que es bastante claro que los *payments* tokens no constituirían ni títulos valores conforme al CCCN, ni valores negociables para la Ley de Mercado de Capitales ^[1158].

Ahora bien, ciertos *utility* tokens, que dan derecho a acceder a servicios o funcionalidades, contienen una obligación irrevocable a una prestación por parte de su emisor. Sin embargo, sería importante estudiar caso por caso los términos y las condiciones específicas del token para determinar si efectivamente esa obligación es incondicional teniendo en cuenta que, en muchos de los casos, la obligación por parte del emisor de permitir el uso de un producto o el beneficio de un servicio está ligada a la efectiva existencia del

producto o servicio desarrollado para el cual los emisores requieren la contribución de quienes compran los tokens [\[1159\]](#).

Respecto a los *security* tokens, sostienen que la representación de un activo, una deuda o una participación en los futuros ingresos, perfectamente podría ser calificada como una obligación incondicional e irrevocable de una prestación, efectuada por emisores, tenedores o por organizaciones unipersonales o sociedades dedicadas en forma exclusiva o parcial al comercio de los mencionados valores negociables: cualquier emisión de tokens sería realizada por algunos de estos actores y realizada por cualquier medio de difusión: al ser la mayoría de las ofertas de tokens realizadas a través de plataformas de Internet, el requisito de difusión se encontraría cumplido [\[1160\]](#).

En consecuencia, calificándose a los *security* tokens como valores negociables con oferta pública, afirman los autores –en opinión que se comparte– que los STOs debieran ser objeto de una regulación específica, de modo tal que (i) no sean asimilados automáticamente a una oferta inicial de acciones o de deuda, (ii) puedan contar con una regulación específica que tenga en cuenta las particularidades de los emisores de este tipo de instrumentos, y (iii) se disminuya la carga regulatoria para empresas de reciente creación que buscan fondear sus negocios y proyectos utilizando herramientas digitales.

Finalmente, Mora y Bericua afirman que tanto la *falta* de regulación como la regulación *defectuosa* pueden tener un efecto letal en el éxito de estas iniciativas que son tan necesarias para el desarrollo de la sociedad y que, en muchos casos, favorecen la inclusión financiera [\[1161\]](#), y se pronuncian, subsidiariamente, por adaptar la normativa que regula el *equity crowdfunding* en Argentina a la emisión de tokens digitales, habida cuenta las similitudes existentes entre ambos fenómenos: en ambos casos se busca financiación, se usan métodos telemáticos para realizar la oferta y la oferta se realiza, en la mayoría de los casos, al público en general [\[1162\]](#) SEP.

3.5.1.3.3.1. La regulación del Equity crowdfunding en Argentina

La regulación del equity crowdfunding en Argentina es reciente ^[1163]. La Ley N° 27.349, publicada en el B.O. el 12/04/17, y conocida como “Ley de Emprendedores”, dedicó 10 artículos a regular los *Sistemas de Financiamiento Colectivo*, a los que aplicó un régimen especial de promoción para fomentar el nacimiento y crecimiento de la industria de capital emprendedor.

Así, la Ley N° 27.349 declara en su Art. 22 que se busca fomentar el financiamiento *de la* industria de capital emprendedor *a través del* mercado de capitales, y dispone que la Comisión Nacional de Valores (CNV) debe reglamentar cómo funcionan estos Sistemas de Financiamiento Colectivo, los que quedan sometidos a la Ley de Mercado de Capitales N° 26.831. Dicha reglamentación fue publicada en Boletín Oficial el 03/01/18, y mediante la Resolución General 717-E/2017 en 56 artículos se reglamentó el Capítulo I del Título II de la Ley 27.349, incorporándose un nuevo Título XIX a las Normas de la CNV (T.O. 2013).

3.5.1.3.3.1.1. Plataformas de financiamiento colectivo. Administración y fiscalización

CNV define a las plataformas de financiamiento colectivo (PFC) como sociedades anónimas que quedan bajo el control estatal permanente de CNV. La actividad de estas sociedades es poner en contacto –de manera profesional y *exclusivamente* a través de *Portales Web*– a una pluralidad de inversores con una pluralidad de *Emprendedores de Financiamiento Colectivo* (según definición del Art. 23, Ley N° 27.349 ^[1164]). CNV no exige un objeto social único y exclusivo, por lo que las PFC pueden realizar otras actividades comerciales, acreditándose por escrito que no existe conflicto de interés entre las otras actividades y la actividad propia de la PFC.

Las PFC son administradas por un directorio, que podrá ser unipersonal o plural según el caso (Ley N° 19.550, Art. 299), y deben designar una persona humana como *Responsable de la PFC* ante CNV, en principio mediante acta de asamblea (Ley N° 27.349, Art. 23). La retribución de este funcionario no puede estar atada a los resultados económicos de la PFC ni a su rentabilidad.

Cualquier hecho ilícito debe ser comunicado de manera fehaciente a este responsable. En caso que CNV cancele la autorización para funcionar, designará a otro Responsable de la PFC. Nótese que las sociedades anónimas que actúan como PFC no pueden prescindir de sindicatura (o en su caso, Comisión Fiscalizadora – Ley N° 19.550:299).

3.5.1.3.3.1.2. Capital social y patrimonio neto mínimo. Contratos. Sistemas

El capital social de la PFC debe estar totalmente integrado al momento de solicitarse la inscripción en CNV, y en toda certificación de sus estados contables anuales deberá surgir un patrimonio neto mínimo de Pesos Doscientos Cincuenta Mil. Los estados contables, junto con la memoria y el acta de asamblea que los aprobó deben acompañarse a CNV anualmente. Cualquier reducción del patrimonio neto mínimo debe ser recompuesta en un plazo de 10 días hábiles. La reglamentación de CNV dispone que tanto los contratos que serán utilizados para *subir* emprendimientos a la PFC como los contratos de inversión a celebrarse con los inversores deben ser presentados a CNV *para su toma de conocimiento*, debiéndose indicar *qué canal se utilizará* para captar y transferir fondos de y hacia los inversores y emprendedores.

Dado que las PFC actúan exclusivamente en la web, CNV exige un detalle de los sistemas informáticos críticos, debiéndose describir el software y hardware utilizados, y los procedimientos de seguridad y contingencia que se seguirán en caso en caso de situaciones fortuitas ajenas a la PFC. Además, un auditor técnico externo debe dictaminar respecto del nivel de seguridad de los sistemas críticos, planes de contingencia y políticas de backup.

3.5.1.3.3.1.3. Guía de selección de Proyectos. Advertencia al inversor y derecho a retractarse. Prohibiciones

Las PFC deben elaborar una guía de selección de Proyectos de Financiamiento Colectivo, donde se contienen los procedimientos de selección y publicación de Proyectos. Dichos procedimientos deben ser objetivos, medibles, razonables y no discriminatorios. También deben informar a CNV los mecanismos que se usan para describir el grado de financiamiento, progreso y/o fracaso de los proyectos publicados por la PFC,

así como para comunicar al inversor aquella información relevante sobre cada proyecto. Finalmente, la PFC debe ofrecer canales de consulta electrónica directa inversor-emprendedor, y establecer un mecanismo de cancelación de proyectos que sean potencialmente fraudulentos.

El Art. 13 del Título XIX de las Normas de CNV obliga a las PFC a exponer en sus publicaciones y en su portal web los riesgos existentes, tanto para Emprendedores de Financiamiento Colectivo como para inversores, aclarándose que ello no implica ni una calificación de riesgo ni una opinión respecto a la factibilidad de los Proyectos de Financiamiento Colectivo (art. 23, Ley N° 27.349) ni asegurar la obtención de lucro al inversor. En particular, la PFC debe informar al inversor:

- i) los tipos de instrumentos de inversión a disposición y los riesgos asociados;
- ii) las restricciones de reventa;
- iii) la información que deben proveer los Emprendedores de Financiamiento Colectivo;
- iv) los límites de la inversión según la Ley N° 27.349;
- v) el plazo de 10 días para retractar la inversión –art. 1110, CCCN [\[1165\]](#) .;
- vi) el resultado del proceso de suscripción del proyecto, y la devolución de la inversión en caso de fracaso de la suscripción.

En desarrollo del art. 31, Ley N° 27.349 las PFC tienen prohibido:

- i) brindar asesoramiento financiero a inversores;
- ii) destacar un Proyecto de Financiamiento Colectivo por sobre otros;
- iii) recibir fondos de Emprendedores de Financiamiento Colectivo para invertirlos en Proyectos de Financiamiento Colectivo desarrollados por ellos mismos;

- iv) gestionar las inversiones en Proyecto de Financiamiento Colectivo, o desviar fondos de un Proyecto a otro;
- v) asegurar el éxito total o parcial de un proceso de suscripción;
- vi) financiar por cuenta propia los Proyectos de Financiamiento Colectivo que publican, incluyendo financiamiento por parte de los controlantes de la PFC;
- vii) asegurar al inversor un retorno sobre su inversión;
- viii) publicar Proyectos de Financiamiento Colectivo desarrollados por el Responsable de PFC o los accionistas de la PFC;
- ix) participar en Proyectos de Financiamiento Colectivo, aún cuando sean publicados por otra PFC; y
- x) publicar una sucesiva suscripción de un mismo Proyecto de Financiamiento Colectivo sin antes notificar a los inversores preexistentes sobre el riesgo de dilución y el derecho de preferencia que les asiste [\[1166\]](#).

3.5.1.3.3.1.4. Identificación de ofertas: transparencia. Comisiones

CNV obliga a las PFC a establecer un sistema que garantice la inalterabilidad de las ofertas ingresadas, que informe el día, hora, minutos, segundos, modalidad, instrumentos, cantidad, precio, individualización del cliente, CUIT/CUIL y toda otra circunstancia que permita identificar la oferta de inversión. Adicionalmente, las PFC deben cumplir las normas de transparencia de la Ley N° 26.831 y del Título XII de las Normas de la CNV. Cualquier situación de gravedad que afecte el adecuado ejercicio de su actividad, obliga a la PFC a abstenerse de funcionar e informar dicha situación a CNV como “Hecho Relevante”.

Las PFC deben publicar todas las comisiones que cobran por sus servicios tanto a inversores como a emprendedores, y mantener esa información actualizada. Deben asimismo incluir una leyenda que informa que CNV no emite juicio sobre los Proyectos de Financiamiento Colectivo, y que la

veracidad de éstos es responsabilidad del Emprendedor de Financiamiento Colectivo. El portal web de la PFC debe incluir, entre otras cosas: (i) una descripción de la guía de selección de Proyectos que se *suben* a la PFC; (ii) el procedimiento de suscripción de los instrumentos de inversión ofertados; (iii) un mecanismo de quejas y reclamos por parte de usuarios; y (iv) información sobre el desempeño histórico de la PFC, indicando porcentajes de incumplimientos, la tasa de morosidad, la definición de cada variable de inversión y su forma de cálculo.

3.5.1.3.3.1.5. Instrumentos de inversión. Mercado secundario. Monto máximo de emisión y de inversión

La Ley de Emprendedores ya estableció que las PFC pueden ofrecer sólo tres instrumentos de inversión: (i) *acciones* a ser emitidas por la sociedad del Emprendedor de Financiamiento Colectivo, si el proceso de suscripción es exitoso; (ii) *préstamos* convertibles en acciones; y (iii) *participación* en un fideicomiso. En cualquier caso, deben informar al inversor sobre los riesgos asociados a cada tipo de inversión (i.e., iliquidez, riesgo de pérdida total, dilución, etc.) y no quedan comprendidos por el régimen de oferta pública de la Ley N° 26.831. El período de suscripción de estos instrumentos no puede ser inferior a 30 días ni mayor a 180 días [\[1167\]](#).

CNV obliga a las PFC a tener una sección dentro de su Portal Web dedicada a la negociación secundaria exclusiva de los instrumentos suscriptos a través de dicho portal, admitiéndose sólo operaciones de contado [\[1168\]](#). En esta sección debe informarse el historial de precios y volúmenes operados desde su suscripción originaria, y en caso de tratarse de préstamos convertibles, debe informarse sobre la fórmula de canje.

En relación al monto máximo de emisión, CNV ha dispuesto que el monto de emisiones acumuladas entre todos los instrumentos emitidos a lo largo de 12 meses por parte de un mismo Proyecto no podrá superar los Veinte Millones de Pesos [\[1169\]](#).

Desde el punto de vista del inversor, existe una doble limitante ya que éstos

no podrán: (i) dentro de un mismo año calendario, invertir importes que superen el 20% de sus ingresos brutos anuales conforme al último ejercicio fiscal cerrado, de lo cual deben dar fe mediante una declaración jurada; y (ii) participar en más del 5% de la suscripción de un Proyecto de Financiamiento Colectivo, o suscribir instrumentos por más de Pesos Veinte Mil, *el que fuere menor*, excepto que se trate de un inversor calificado [\[1170\]](#)

3.5.1.3.3.1.6. Información sobre el Proyecto de Financiamiento Colectivo. Cambio material en el Proyecto

El Emprendedor de Financiamiento Colectivo debe ser un “emprendimiento argentino” según reglamentación del Ministerio de Producción, y los socios e integrantes de los órganos de administración y fiscalización de la SA o SAS a ser constituida (o el fiduciario, en caso de constituirse un fideicomiso) no deben estar incurso en incompatibilidades e inhabilidades determinadas por CNV [\[1171\]](#). La PFC debe asegurar al inversor la constitución del vehículo (SA, SAS o fideicomiso) en el plazo aplicable en caso de suscripción exitosa.

Respecto de cada Proyecto de Financiamiento Colectivo, toda PFC deberá recabar determinada información según se emplee una SA [\[1172\]](#), una SAS [\[1173\]](#) o un fideicomiso [\[1174\]](#), y en cualquier caso debe publicar:

- i) una descripción del proyecto y de su plan de negocio redactada en lenguaje plano;
- ii) el número total de empleados, si los hubiere;
- iii) una sección en la que se expliquen los riesgos generales de inversión;
- iv) el monto de emisión buscado y la fecha límite de suscripción, incluyendo una declaración de que si no se alcanza la suma pretendida no habrá emisión y se retornarán los fondos recaudados. En caso de deducirse cualquier costo en concepto

de gasto, el monto o porcentaje que se deducirá deberá ser informado;

v) la posibilidad de los emprendedores de aceptar ofrecimientos excedentes del monto a suscribir y, si es así, el monto máximo de sobre suscripción –el cual nunca podrá superar el veinticinco por ciento (25%) del monto original– y el mecanismo de cómo se alojará la sobre-suscripción y qué destino se dará a los fondos que eventualmente pudieren exceder el monto originalmente previsto;

vi) una descripción razonablemente detallada de la finalidad que los emprendedores le darán a los fondos producto de la suscripción, con información suficiente. Si son varias finalidades, tienen que describir cada una y explicar bajo qué circunstancias se alojarán los fondos a cada finalidad. Los fondos producto de la suscripción deberán ser utilizados en el desarrollo de la actividad del Proyecto. No podrán ser utilizados para reorganizaciones societarias, adquisición de otras empresas o concesión de créditos a terceros así como valores emitidos por otras sociedades;

vii) descripción del tipo y la clase de los instrumentos ofertados. Si hubiere, las garantías aportadas;

viii) el precio de los instrumentos o la metodología para su determinación constando que antes de cualquier venta de instrumentos, cada inversor recibirá por escrito el precio final;

ix) descripción de los derechos vinculados a los instrumentos y su forma de ejercicio, incluida cualquier limitación de esos derechos. Se incluirá información sobre la amortización y remuneración de los mismos o su forma de cálculo cuando no sea posible publicarla con anterioridad, pactos de recompra y limitaciones a la venta;

x) una descripción de los términos materiales de cualquier endeudamiento del Emprendedor de Financiamiento Colectivo, incluyendo tasa de interés, maduración y cualquier

otro término material;

xi) una descripción de las emisiones de financiamiento colectivo realizadas en los últimos tres años, incluyendo la fecha de emisión, una descripción de la misma, de los instrumentos ofrecidos y del monto colocado;

xii) una descripción de cualquier transacción realizada en el último año fiscal o actualmente propuesta por un monto igual o mayor al 5% del monto agregado recaudado a través de emisiones de financiamiento colectivo de los últimos 12 meses (incluyendo la suscripción a ser emitida) en la que participa o tiene interés (directo o indirecto) un director o gerente; un accionista final con más del 20% de los votos y familiares hasta el tercer grado de consanguinidad de los anteriores;

xiii) una descripción de la situación financiera del emprendedor incluyendo liquidez, recursos de capital y el historial de los resultados de las operaciones;

xiv) presentación de los estados contables anuales de hasta los últimos tres años –realizados según las normas contables argentinas– de la sociedad o del fideicomiso que sirva de vehículo para la inversión en el Proyecto de Financiamiento Colectivo, con firma de contador independiente certificada por el CPCE;

xv) cualquier otro hecho y circunstancia que consideren relevantes para los potenciales inversores y para entender el negocio;

xvi) reconocer en el estatuto social: (a) el derecho de los inversores de participar en las asambleas o reuniones de socios; (b) el derecho de representación en la asamblea o reunión de socios conforme la legislación vigente; (c) que, en el caso de que la figura de inversión sea una SA o una SAS, los acuerdos de accionistas que tengan por objeto el ejercicio del derecho de voto en las asambleas o reuniones de socios o que incidan de algún modo en la transmisibilidad de las acciones,

participaciones sociales u otros instrumentos representativos de capital habrán de ser comunicados inmediatamente a la propia sociedad y por esta al resto de socios; y

xvii) si alguna vez el Emprendedor falló en completar los requerimientos enumerados anteriormente.

Debe destacarse que cualquier cambio material en el Proyecto de Financiamiento Colectivo durante el período de suscripción debe ser informado por el Emprendedor a la PFC, quien a su turno debe comunicarlo a los inversores que hayan suscripto instrumentos de inversión. Los inversores tienen 5 días para *ratificar* su participación, caso contrario se les devuelve la inversión [\[1175\]](#).

En todos los casos, el contrato celebrado entre la PFC y el Emprendedor deberá prever la permanencia del Proyecto en el Sistema de Financiamiento Colectivo por un plazo mínimo que abarque hasta la primera presentación de los Estados Contables correspondientes al ejercicio económico posterior a la suscripción exitosa mediante el Sistema de Financiamiento Colectivo.

Durante dicho plazo, el Emprendedor debe entregar a la PFC [\[1176\]](#): (i) la memoria; (ii) estados contables; (iii) copia del acta del órgano de administración que los aprobó; (iv) informe del síndico [\[1177\]](#); y (v) una actualización de cierta información publicada inicialmente.

Adicionalmente, el Emprendedor debe publicar trimestralmente en la PFC un informe sobre la evolución del Proyecto, que, como mínimo, debe contener una comparación entre el Plan de Negocios presentado en su momento y el nivel de avance en el cumplimiento del mismo, y si se detectan desvíos durante la implementación del Plan de Negocios, los mismos deberán ser informados por las PFC a la CNV. También debe incluirse una comparación entre el Plan de aplicación de fondos presentado a la PFC y el nivel de ejecución del mismo, informándose los desvíos detectados por la PFC a la CNV. Este informe trimestral debe también informar cualquier variación significativa en la estructura de financiamiento del Proyecto.

3.5.1.3.3.1.7. Importancia del Equity Crowdfunding

La SEC recientemente publicó un estudio en el que afirma que *el crowdfunding está proveyendo una nueva fuente de financiación para emprendedores y PYMES, quienes de otra manera no habrían tenido acceso a financiamiento usando canales alternativos* [\[1178\]](#). En efecto, en el período comprendido entre Mayo y Diciembre de 2016, 156 empresas colocaron 163 emisiones por un total de 10 Millones de Dólares.

En esencia, la regulación del *crowdfunding* en EE.UU impulsada por la SEC en cumplimiento de una ley de 2012 conocida como *Jumpstart Our Business Startups* (conocida como Ley JOBS) no es muy distinta de la regulación de la CNV, y de hecho contempla un límite máximo de emisión de 1 Millón de Dólares – *mutatis mutandis* aprox. 20 Millones de Pesos, al tipo de cambio a la época de la reglamentación bajo estudio–.

Sin embargo, podría sostenerse que en su tarea reglamentadora la CNV ha establecido en el art. 56 del Título XIX de sus Normas un techo muy bajo (AR\$ 20.000,00) que podría dificultar el florecimiento de las PFC en la República y también el acceso al financiamiento de nuevas empresas que, generalmente, no son aún sujeto de crédito bancario y a lo sumo han recibido leves fondeos *FFF*.

Si bien es usual que el poder de policía financiero no permita grandes inversiones en proyectos *subidos a* PFCs debido al alto riesgo asociado a este tipo de inversión [\[1179\]](#), sería recomendable subir el techo fijado por el art. 56 y atarlo a una variable dinámica [\[1180\]](#).

De otro costado, es previsible que se repliquen aquí las críticas que se han generado en EE.UU con motivo de los amplios deberes de información impuestos al Emprendedor, aunque no puede negarse que los informes trimestrales exigidos por el art. 50 del Título XIX sólo obligan a llevar una adecuada contabilidad de gestión, y eso es bueno tanto para el emprendedor como para el inversor, y se trata de métricas que más tarde o más temprano serán exigidas por potenciales inversores de mayor envergadura. En fin, se trata de la profesionalización del *management* que es coherente con un deber

de diligencia del buen hombre de negocios que ya es exigible por el art. 59 de la Ley N° 19.550 (y por el art. 1674 del CCCN para el caso del fiduciario).

3.5.1.3.3.1.8. *Quid de la aplicabilidad de la regulación del equity crowdfunding a los Security Token*

Se señaló antes que en EE.UU se están aplicando las regulaciones del equity crowdfunding a ciertos tipos de STOs [\[1181\]](#), permitiendo captar hasta 1.7 millones de Dólares, pero el comprador del token debe retenerlo por 12 meses obligatoriamente.

Junto con Mora y Bericua, se sostiene que debería revisarse la posibilidad de cumplimiento no solo por parte de los emisores sino también por parte de las plataformas en las que se ofrecen estos instrumentos y si los perfiles de inversores a los que accederían serían adecuados para poder obtener el financiamiento necesario.

Afirman los autores citados que sería interesante analizar si sería posible una oferta que utilice dos tipos de regulaciones vigentes para poder acceder a dos tipos de perfiles de inversores diferentes, por ejemplo, la regulación de *crowdfunding* para el denominado *retail* y el panel PyMES para inversores *calificados*. Adicionalmente, entienden los autores citados que el White Paper que se emite como documento informativo acerca del token y del proyecto podría cumplir con los requisitos establecidos por el regulador para los prospectos requeridos en el caso de las emisiones de PyMES [\[1182\]](#) y también podrían adaptarse las regulaciones sobre registros de valores negociables para darle al sistema de registro compuesto por la *blockchain* y los monederos la misma validez que los sistemas de registro electrónico que se utilizan en la actualidad [\[1183\]](#).

3.5.1.4. *Blockchain Federal Argentina (BFA): BaaS*

Vistas las opciones posibles de caracterización jurídica de los criptoactivos según cada especie del género, antes de proseguir con la caracterización

jurídica de los contratos inteligentes para el derecho argentino, nos detendremos en el estudio de una interesante plataforma de *Blockchain* recientemente lanzada en Argentina en Ethereum ^[1184], auspiciada por decenas de instituciones, empresas y organismos nacionales y provinciales ^[1185], con la intención de ser la primera infraestructura de este tipo a escala federal que puede ser utilizada por cualquier ciudadano, y es pionera en la región por el hecho de sostener una plataforma de *blockchain* a partir de un aporte multisectorial ^[1186].

Así, se destaca que en BFA, que es una *blockchain* permitida ^[1187], todas las partes que conforman la organización participan en la toma de decisiones, así como también pueden hacerlo en los aportes tecnológicos, y que el resultado de este modelo es una infraestructura de *Blockchain* que requiere un bajo costo de procesamiento y donde no es necesario que exista una criptomoneda circulante ^[1188], ya que su uso es público y gratuito. En efecto, las organizaciones que deseen desarrollar servicios y/o aplicaciones sobre BFA solo deben aceptar un acuerdo de utilización y buenas prácticas, pero no están obligados a contribuir con la infraestructura. Al definirse como proveedor de un servicio de confianza, BFA es responsable del mantenimiento de esa infraestructura para que todos los usuarios puedan disponer del mejor ambiente para desarrollar servicios o volcar aplicaciones ^[1189].

3.5.1.4.1. Miembros de BFA. Modelo participativo e ingeniería organizacional

Con representantes de la industria y el comercio, la academia, la administración pública nacional, los gobiernos provinciales y la sociedad civil, BFA se potencia a través de las contribuciones de cada uno de sus participantes, asumiendo un marco de colaboración que atraviesa todos los procesos de toma de decisiones, con un modelo de Prueba de Autoridad (PoA) ^[1190].

Así, se trata de una iniciativa colaborativa que se potencia a través de los aportes de decenas de instituciones multisectoriales que trabajan en conjunto en torno a un modelo de gobernanza abierto y participativo [\[1191\]](#).

Se ha señalado que dada la cantidad de implementaciones de *Blockchain* que existen actualmente en el mundo, BFA podría haber tomado otras formas: (i) una *blockchain* gubernamental cerrada o (ii) una *blockchain* pública intermediada por la circulación de criptomoneda. Pero se optó por un modelo gratuito [\[1192\]](#) y que reafirme la participación de las múltiples partes interesadas en su conjunto [\[1193\]](#).

De acuerdo a su ingeniería organizacional, se ha remarcado que existen dos formas de participación en BFA: (i) como *usuarios* del servicio o como (ii) *partes* de la organización. Los usuarios, por una parte, pueden desarrollar y volcar sus propias aplicaciones en la red, enviar transacciones y desplegar los nodos necesarios para hacerlo, todo de forma gratuita. De otro costado, las *partes* de BFA son aquellas empresas, instituciones u organizaciones que, habiendo firmado un contrato de colaboración, participan en la toma de decisiones respecto al futuro de la iniciativa. Todas ellas tienen las mismas facilidades que los usuarios a la hora de desarrollar aplicaciones e instalar nodos transaccionales, pero también tienen la opción —no la obligatoriedad— de contribuir a la infraestructura de la red [\[1194\]](#).

3.5.1.4.2. Almacenamiento *off-chain*

Finalmente, como característica saliente, y anticipándose a las dificultades específicas del llamado *derecho al olvido* que se analizan más abajo [\[1195\]](#), en BFA el almacenamiento de información es *off-chain*: la plataforma no funciona como una nube para almacenar archivos sino que cada aplicación que corre sobre la plataforma es responsable de ellos. En el registro de BFA solo se almacenan los digestos criptográficos —los *hashes*— de esos archivos. Los usuarios —es decir, los proveedores de servicios—, son responsables de almacenar la información de la manera que consideren más adecuada, pero al

tener los digestos criptográficos sellados en la *blockchain* encuentran la forma de demostrar que sus documentos no fueron modificados luego de que ese *hash* se obtuvo ^[1196].

3.5.1.5. Contratos inteligentes: su recepción legal en Argentina

Habiendo analizando las posturas sobre la naturaleza jurídica de cada especie de criptoactivo según su específica funcionalidad subyacente (i.e. pago/inversión/acceso), corresponde ahora analizar el tratamiento de los contratos inteligentes bajo la legislación argentina.

3.5.1.5.1. Contratos inteligentes como contratos electrónicos

En línea con la opinión del autor español Legerén-Molina ^[1197], Mora –en opinión que comparto– afirma que los contratos inteligentes son una *modalidad de los contratos electrónicos* ^[1198].

En este sentido, postula Mora que la validez de los contratos electrónicos se admite hace años ya, en base a las equivalencias entre documentos materiales y digitales, la validez de las firmas electrónicas y las equivalencias entre firmas ológrafas y digitales, dispuestas en nuestro país a partir de la Ley de Firma Digital y luego ratificadas por el CCCN en sus Arts. 286 ^[1199], 287 ^[1200], 288 ^[1201], 319 ^[1202], 1106 ^[1203], 1107 ^[1204], 1109 ^[1205], 1110 ^[1206] y 1020 ^[1207].

También afirma Mora que el análisis de la imputabilidad de una declaración de voluntad emitida automáticamente por medio de computadoras tampoco es nuevo, siendo aplicables las mismas consideraciones dadas en relación a las técnicas de Intercambio Electrónico de Datos, o *EDI*, según siglas en inglés.

En línea con el pensamiento de Mora, también se pronuncia

Chomczyk^[1208] afirmando que no existe norma legal en Argentina que prohíba a los particulares usar contratos inteligentes para celebrar e instrumentar contratos, y que la única limitación vendrá dada por aquellos casos en los que el tipo de relación jurídica que se pretenda instrumentar exija el cumplimiento de ciertas formalidades bajo pena de nulidad del acto subyacente, o simplemente configurando una promesa de realizar el acto en cuestión con las formalidades requeridas^[1209], i.e., contratos formales.

Así, afirma Chomczyk que si el tipo de contrato lo permite, no habrá obstáculo para que las partes instrumenten en el software su consentimiento para crear, regular, modificar, transferir o extinguir una relación jurídica^[1210], y agrega que al regir la libertad de formas, deberá analizarse si el soporte electrónico es idóneo para cumplimentar el requisito de escritura que se exige para varios de los contratos tipificados por el CCCN.

En este sentido, Chomczyk analiza teleológicamente los arts. 284, 286 y 288 del CCCN que a continuación se transcriben:

“Art. 284, CCCN.- Libertad de formas. Si la ley no designa una forma determinada para la exteriorización de la voluntad, **las partes pueden utilizar la que estimen conveniente**. Las partes pueden convenir una forma más exigente que la impuesta por la ley.

Art. 286, CCCN.- Expresión escrita. La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. **Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos.**”

Art. 288, CCCN.- Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo.

En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento.” (el resaltado es mío).

Y concluye que, de la lectura atenta de ambas normas, puede colegirse que “*los smart contracts podrían ser contratos en sentido legal puesto que la instrumentación mediante software es viable*” [\[1211\]](#).

En punto a la forma de firmar contratos inteligentes, afirma el autor citado que si bien el Art. 288 CCCN menciona la *firma digital* para instrumentos generados por medios electrónicos, existe cierta doctrina que sostiene que la previsión del Art. 288 admitiría *todo* tipo de firma, ya sea digital o *electrónica*, en tanto sea capaz de asegurar indubitablemente la autoría e integridad del documento [\[1212\]](#). En este sentido, afirma Chomczyk –en opinión que se comparte– que el CCCN no ha derogado a la ley especial –i.e, Ley de Firma Digital–, por lo cual el régimen especial está vigente, y por ende un instrumento generado por medios electrónicos puede ser firmado con firma electrónica, aunque al no ser ésta una firma *digital*, existirá siempre el riesgo de su desconocimiento, y la necesidad de probar judicialmente su autoría por cualquier medio [\[1213\]](#).

En este sentido, señala Chomczyk que la cuestión sobre el uso de firmas electrónicas o digitales no es menor, puesto que la gran mayoría de las plataformas usadas para contratos inteligentes que existen hoy hacen uso de firmas electrónicas más o menos complejas desde el punto de vista técnico [\[1214\]](#). Precisa también el autor citado que en muchos casos, los contratos inteligentes estarán sujetos a las normas que regulan los contratos celebrados por adhesión a cláusulas generales predispuestas [\[1215\]](#), las que se analizan más abajo.

Finalmente, Santarelli [\[1216\]](#) afirma que el art. 284 CCCN viene preconizando para los actos jurídicos en general, el principio de libertad de formas, y exhibe la plasticidad y apertura de su régimen al darle cabida a la

distinción entre documentos particulares firmados y no firmados, incluyendo en tal categoría a *“todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información”*. Afirma el autor citado que con igual sesgo, el art. 288 CCCN define la firma, sus funciones, y admite a la firma digital, en tanto *“asegure indubitablemente la autoría e integridad del instrumento”*. Agrega Santarelli que en materia contractual, se ratifica en el art. 1015 CCCN el principio de libertad de formas y se dispone en art. 1019 CCCN, que regula las reglas de la prueba de los contratos, una clara apertura en cuanto a la elegibilidad de formas, lo que permite sostener que el CCCN admitiría a acuerdos que puedan expresarse sobre códigos de programación en lenguaje no natural ^[1217]. También precisa Santarelli, con mucha razón, que en los contratos de consumo la utilización de medios electrónicos recibe su propia regulación en art. 1106, CCCN respecto de la utilización de medios electrónicos, al establecer *“siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un soporte electrónico u otra tecnología similar”*. Invoca también el art. 1107, CCCN que establece que *“si las partes se valen de técnicas de comunicación electrónica o similares para la celebración de un contrato de consumo a distancia, el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos.”* Acota Santarelli que el ordenamiento jurídico concibe y admite entonces la utilización de soportes distintos a los usuales, en la medida que estén debidamente informados, por lo que puede concluirse que un contrato autoejecutable, celebrado en lenguaje informático, no natural, es, con las prevenciones efectuadas, legalmente viable, así sea un contrato entre partes, como de adhesión, o de consumo.

3.5.1.5.2. El contrato inteligente como contrato celebrado por adhesión

Le asiste razón a Chomczyk cuando destaca que la práctica actual en materia de *Smart Contracts* denota la imposición de software de una parte a la

otra, donde una de las partes es quien impone a la otra el software que receptorá los derechos y obligaciones pactados entre las partes, sin dar posibilidad de discutir la redacción o programación del contrato inteligente. Como consecuencia de ello, es posible considerar a estos contratos inteligentes como contratos con cláusulas predispuestas, aquéllos regulados en el art. 984 y siguientes del CCCN:

“Art. 984, CCCN.- Definición. El contrato por adhesión es aquel mediante el cual uno de los contratantes adhiere a cláusulas generales predispuestas unilateralmente, por la otra parte o por un tercero, sin que el adherente haya participado en su redacción.”

3.5.1.5.2.1. El contrato adhesivo

Andrés Sánchez Herrero ^[1218] analiza la figura del contrato por adhesión y señala que son contratos caracterizados por el modo en que se celebran ^[1219], sin que el *nomen iuris* implique que haya en su contenido contractual algo distinto, sino solo una forma particular de arribarse al consentimiento contractual. En efecto, *al ser contratos celebrados por adhesión* de una de las partes contratantes, el *aceptante o adherente* ^[1220] no ha participado en la configuración de su contenido ni en su ideación ^[1221]. Se agrega que la redacción puede haber estado a cargo del predisponente –o estipulante–, o de un tercero, pero lo dirimente no es que una de las partes predisponga el contrato, sino que la otra debe adherir a esa propuesta, sin chistar ^[1222].

Otra nota característica de los contratos por adhesión es la presencia de cláusulas generales, aquéllas pensadas para regular una contratación en masa, y no para un caso particular, y que, además no son cláusulas negociables. Puede existir adhesión sin cláusulas generales predispuestas, y en éste caso, no se aplicará lo dispuesto en los art. 984 y siguientes del CCCN ^[1223]. Se señala

también que el adherente o aceptante puede ser o no ser un consumidor [\[1224\]](#), y que quien contrata por adhesión, tiene prácticamente anulada su libertad contractual, pero no su libertad de contratar [\[1225\]](#).

3.5.1.5.2.2. *Requisitos de las cláusulas generales predispuestas*

Dispone el art. 985, CCCN:

“Requisitos. Las cláusulas generales predispuestas deben ser comprensibles y autosuficientes.

La redacción debe ser clara, completa y fácilmente legible.

Se tienen por no convenidas aquellas que efectúan un reenvío a textos o documentos que no se facilitan a la contraparte del predisponente, previa o simultáneamente a la conclusión del contrato.

La presente disposición es aplicable a la contratación telefónica, electrónica o similares.” (el resaltado es mío).

Señala Andrés Sánchez Herrero que las cláusulas generales deben ser comprensibles y autosuficientes, y la redacción ser clara, completa y fácilmente legible [\[1226\]](#). Las cláusulas generales deben ser comprensibles para el aceptante, y su redacción, clara y fácilmente legible, lo que obliga a evitar términos técnicos [\[1227\]](#), pero no obliga a usar un idioma en particular, y la redacción debe ser autosuficiente: cualquier reenvío a textos que no se entregan al momento de aceptarse el contrato, se tiene por no efectuado [\[1228\]](#).

Ahora bien, el tercer párrafo del art. 985 CCCN declara que las reglas expuestas se aplican *a la contratación telefónica, electrónica, o similares*, lo que permite sin más sostener que un contrato inteligente, redactado por un predisponente, debiera cumplir las pautas del art. 985, CCCN.

3.5.1.5.2.3. Interpretación del contrato por adhesión

La pauta interpretativa de estos contratos dispone que las cláusulas *ambiguas* se interpretan en contra del predisponente y a favor del adherente, lo que requiere que una cláusula tenga al menos más de un sentido interpretativo válido [\[1229\]](#), sin importar si ello se debe a una actitud accidental o deliberada.

3.5.1.5.2.4. Cláusulas particulares en el contrato por adhesión

Las cláusulas particulares son aquellas que, negociadas individualmente, amplían, limitan, suprimen o interpretan una cláusula general. En caso de incompatibilidad entre cláusulas generales y particulares, éstas prevalecen.

3.5.1.5.2.5. Cláusulas abusivas en el contrato por adhesión

El art. 988 CCCN dispone:

“Cláusulas abusivas. En los contratos previstos en esta sección, **se deben tener por no escritas:**
las cláusulas que desnaturalizan las obligaciones del predisponente; ^[SEP]
las que importan renuncia o restricción a los derechos del adherente, o amplían ^[SEP] derechos del predisponente que resultan de normas supletorias; ^[SEP]
las que por su contenido, redacción o presentación, no son razonablemente previsibles.” (El resaltado es mío).

Como regla general, se afirma que es abusiva la cláusula que provoca un desequilibrio significativo entre los derechos y obligaciones de las partes, en perjuicio del adherente [\[1230\]](#). Como reglas particulares, se considera abusiva la cláusula que desnaturaliza las obligaciones del predisponente, o que implica

renuncia o restricción de los derechos del adherente, o la ampliación de los derechos del predisponente, o la cláusula *sospresiva*. Se ha señalado que la abusividad depende del desequilibrio significativo entre derechos y obligaciones que puede (o no) causar un perjuicio al adherente en un caso concreto, y no en abstracto. Así, la supresión de un derecho del adherente podría ser, en abstracto, considerada abusiva, pero si en el caso concreto, tal supresión es compensada con la ampliación de otro derecho a favor del adherente, o con la restricción de algún derecho del predisponente, no habría tal abusividad, por aplicación analógica del art. 1119, CCCN [\[1231\]](#).

La cláusula sorpresiva, a su turno, es aquella que por su contenido, redacción o presentación no es razonablemente previsible, y ello perjudica al adherente [\[1232\]](#). Lo propio de este tipo de cláusula abusiva es la violación del deber de transparencia [\[1233\]](#), y a diferencia de los supuestos anteriores, en la cláusula sorpresiva no es el contenido lo abusivo, sino la forma desleal de comunicar el contenido, de presentar la cláusula –lo que permite pensar cláusulas que son doblemente abusivas, por su contenido y por su forma de presentación, lo que es normal: se tiende a querer ocultar el abuso [\[1234\]](#).

Ahora bien, la cláusula sorpresa no debe ser *razonablemente previsible*, lo que implica analizar la previsibilidad de la cláusula desde el punto de vista del adherente. Esto genera cinco consecuencias. La primera: *a contrario sensu*, la cláusula efectivamente prevista por el adherente no será una cláusula sorpresiva y abusiva. La segunda: debe exigirse un cierto grado de comportamiento diligente en el adherente, lo que obligará siempre analizar las circunstancias del caso concreto [\[1235\]](#). La tercera: será sorpresiva la cláusula que se aparta de las cláusulas usuales en el ramo, o de lo que fue la negociación o conversación previa a celebrarse el contrato. La cuarta: la forma de redacción, el lenguaje utilizado, puede volver sorpresiva a una cláusula. La quinta: la forma de presentación de una cláusula en sí, su ilegibilidad, su ubicación dentro del clausulado contractual, el título inadecuado, son todos factores que pueden volver abusiva una cláusula por sorpresiva.

Finalmente, con gran precisión señala Andrés Sánchez Herrero que lo previsto en el art. 988 CCCN no sólo se aplica al contrato por adhesión a

cláusulas generales predispuestas, sino también (i) al contrato celebrado por adhesión a cláusulas predispuestas no generales, y (ii) al contrato con cláusulas predispuestas, pero no celebrado por adhesión [\[1236\]](#).

3.5.1.5.2.6. Problemática del contrato inteligente como contrato adhesivo

Afirma Chomczyk que considerar al contrato inteligente como contrato celebrado por adhesión traería dos problemas: (i) si el texto del contrato está circunscripto al código, podría haber un incumplimiento del párrafo 2 del Art. 985 del CCCN, por la falta de claridad y facilidad de lectura propia del lenguaje de programación; y (ii) estaría abierta la posibilidad de la declaración de nulidad de ciertas cláusulas que sean consideradas abusivas [\[1237\]](#).

En este sentido, afirma Chomczyk que un juez podría estimar que: (a) el contrato no es *Smart Contract* por no reunir estos elementos de claridad y transparencia; y (b) debe integrar el contrato con elementos adicionales fuera del código, tornando todo el esfuerzo de autosuficiencia del contrato inteligente en una actividad superflua. En particular, el problema con la integración judicial del contrato inteligente radica en cómo hacer que esta orden judicial sea seguida por el protocolo que gobierna al contrato inteligente [\[1238\]](#).

Evidentemente, la respuesta a los interrogantes que con razón plantea Chomczyk no puede darse en abstracto, y sólo podrán responderse atendiendo a los siguientes factores:

- i) a las circunstancias específicas de las personas involucradas, el tiempo y el lugar, incluyendo la imprudencia, la negligencia y la impericia profesional,
- ii) el significado específico dado a las palabras empleadas en el contrato, salvo que deban entenderse en el sentido que les da el uso general,
- iii) el deber de obrar con prudencia y pleno conocimiento de las cosas, y la consecuente diligencia exigible al agente, así

como la valoración de la previsibilidad de las consecuencias de los contratos inteligentes en entornos *on-chain*,

iv) si existe (o no) una confianza especial, y si se debe tener en cuenta la naturaleza del acto y las condiciones particulares de las partes,

v) si es posible invocar (o no) un error esencial de parte del adherente, incluyendo el error en:

a. la naturaleza del acto,

b. si existe un resultado diverso o de distinta especie que el que se pretendió contratar, o una calidad, extensión o suma diversa a la querida,

c. o si la cualidad sustancial de un servicio o bien específico ha sido determinante de la voluntad jurídica según la apreciación común o las circunstancias del caso y, muy especialmente, ^[L]_[SEP]

d. si los motivos personales relevantes han sido (o no) incorporados expresa o tácitamente al contrato,

e. si la persona con la cual se celebró el contrato inteligente, o a la cual se refiere el mismo, fue (o no) determinante para su celebración,

vi) si se trata de un error de cálculo, y en su caso, si ha sido (o no) determinante,

vii) si se cumplió (o no) con el deber de prevención y de evitar causar un daño no justificado, o si se tomaron medidas para disminuir su magnitud o no agravar el daño causado, y

viii) las negociaciones preliminares, la conducta posterior de las partes, y la naturaleza y finalidad propias de los contratos inteligentes.

Criptoactivos, Contratos Inteligentes vs. Estados Contables ¿Activo, Pasivo o Patrimonio Neto? [\[1239\]](#)

3.5.1.6. *Es interesante también analizar el reflejo contable de los criptoactivos y del efecto de sus transacciones mediante contratos inteligentes. La materia, en éste ámbito como en otros, se está desarrollando rápidamente.*

La IFRS publicó un working paper en Noviembre de 2018 ^[1240], actualizado en unas Directrices publicadas en Junio de 2019 ^[1241], donde en líneas generales propuso el tratamiento para el emisor y para el tenedor de tokens, en base a la siguiente clasificación. Debe repararse que, sin embargo, dichas directrices o comentarios de la IFRS no constituyen un *estándar* contable, lo cual deja abierto el tratamiento de los criptactivos a cada caso concreto, vinculando todos los estándares precedentes y buscando el encuadramiento en ellos.

3.5.1.6.1. *Criptomonedas*

Si bien pueden ser consideradas como un medio general de intercambio con las mismas características que las monedas convencionales, la IFRS considera que las criptomonedas no son un activo financiero equiparable al dinero ^[1242]. La tenencia de criptomonedas con fines de comercialización en el curso ordinario de los negocios debería, en principio, ser tratada como un bien de cambio, de acuerdo a la *IAS 2 Inventories* ^[1243]. La tenencia de criptomonedas con otro fin distinto a su comercialización, debe ser tratada como tenencia de un activo fijo intangible, de acuerdo a la *IAS 38 Intangible Assets* ^[1244].

3.5.1.6.2. *Taxonomía del token y opciones de reflejo contable*

En 2018, la IFRS ^[1245] analizó las diferencias entre una Initial Coin Offering (ICO) y un Token Generating Event (TGE). Afirmó que en una ICO, el token se emite *antes* de que la entidad emisora haya desarrollado los

bienes o servicios prometidos [\[1246\]](#), mientras que en un TGE, el token se emite *después* de haber desarrollado los bienes o servicios [\[1247\]](#). Evidentemente, cuando estamos frente a un TGE, la venta de tokens puede, en algunos casos, generar ingresos por ventas a clientes [\[1248\]](#), pero la situación puede ser muy distinta con las ICOs.

La emisión –i.e, creación– de ICOs genera, generalmente para el emisor, un incremento de su activo, a través de dinero u otras criptomonedas. Ahora bien, deberán analizarse los derechos que el token confiere en su *White Paper* para poder determinar su correcto encuadre contable en el pasivo del emisor [\[1249\]](#).

En este sentido, según los términos de creación del token, su reflejo contable podrá impactar en distintos lugares del balance: (i) en el patrimonio neto –si el token vendido es asimilable a una acción o similar participación social, es decir, es un security token–; (ii) en el pasivo –si el token vendido genera una obligación del emisor a entregar un bien o servicio *actual o futuro*, se incluyen aquí los utility tokens propiamente dichos–; o (iii) sólo en el activo –si el token vendido genera ingreso de caja, sea en moneda convencional, sea en otras criptomonedas y no genera ninguna obligación adicional para el emisor, es decir, los casos de venta de asset tokens [\[1250\]](#).

3.5.1.6.2. *Utility tokens*

Son activos digitales que otorgan un derecho de acceso futuro a ciertos bienes y servicios ofrecidos por el emisor, pero no confieren un derecho de propiedad. Son comercializados vía ICOs.

En estos casos, el emisor de una ICO está obligado a desarrollar una actividad para poder cumplir lo prometido, y ello es contablemente un pasivo, no financiero, que debe ser debidamente provisionado dado que cumplidas ciertas condiciones fijadas en el *White Paper*, el emisor deberá entregar/permitir el acceso a lo prometido, en el momento pactado [\[1251\]](#).

3.5.1.6.3. Asset tokens

Son activos digitales vendidos en TGEs, que otorgan al tenedor del token un derecho actual de propiedad para adquirir o usar un bien o un servicio ya existente, a título de dueño. Su reflejo contable sería el menos complicado, ya que impacta en el activo corriente del emisor. Sólo si el servicio o bien funciona mal, y genera una responsabilidad exigible por el tenedor del token, entonces procederá reflejar en el pasivo del emisor esta provisión.

3.5.1.6.4. Security tokens

Son activos digitales que representan un interés económico en la organización que los emite, que puede incluir el derecho a una participación en los ingresos a ser generados, o a recibir participaciones sociales a ser emitidas por la organización que los emite, o el derecho a votar en la toma de decisiones de la organización que los emite, y también, por qué no, el derecho a percibir una renta fija en el tiempo como otros instrumentos de deuda, i.e. un pasivo financiero de acuerdo a la definición de la NIC 32. Para estos casos, aplican en general las normas IFRS IAS 32 [\[1252\]](#).

En este sentido, la creación y venta de security tokens –STOs– puede ser considerada como *activos financieros* que prometen a su tenedor el derecho a recibir participaciones sociales, pagos de dividendos, o incluso futuras participaciones a ser emitidas –todo dependerá de los términos contenidos en White Paper–, generando la consecuente obligación contractual en el emisor de entregar dinero o participaciones, con lo cual, luce adecuada su caracterización como instrumentos financieros, y así deberían ser contablemente tratados [\[1253\]](#).

Aquí, el punto dirimente será que el token no garantice a su tenedor una ganancia, sino solo la participación en un resultado eventual. Si éste es el caso, estos tokens se reflejan contablemente en el patrimonio neto del emisor [\[1254\]](#), y tendrían un tratamiento análogo *mutatis mutandis* al de una

ampliación de capital mediante emisión de participaciones sociales [\[1255\]](#).

Si, por el contrario, los términos de creación de un security token expuestos en el White Paper *garantizan* a su tenedor una determinada rentabilidad, medida en dinero, o le confieren una opción de rescate, aún cuando puedan ser necesarias ciertas y determinadas condiciones que no dependan del emisor, entonces este tipo de security tokens puede ser considerado un pasivo no corriente [\[1256\]](#), financiero [\[1257\]](#). Aquí lo dirimente será que el emisor no tenga opción de entregar dinero, o, en su caso, participaciones sociales por ejercicio de un derecho de conversión [\[1258\]](#).

Ahora bien, como ocurre también *off-chain*, el valor negociable emitido puede tener ambos componentes y ser asimilable a una participación social *-equity-* y también a un instrumento de deuda *-debt-*, lo que implica que el token deberá ser analizado en profundidad para evaluar el tratamiento contable pertinente [\[1259\]](#).

3.5.1.6.5. Tokens híbridos

Son activos digitales que combinan las características de los utility, asset y security tokens. Su reflejo contable dependerá del análisis, caso por caso, de las condiciones de su creación.

3.5.1.7. Contratos Inteligentes vs. Estatuto del Consumidor

Sin dudas, uno de los campos en los que más fricción producirá la implementación de los contratos inteligentes es en el ámbito del Estatuto del Consumidor, la disciplina con mayor fuerza expansiva dentro del Derecho Privado.

Se ha sostenido que los derechos de los consumidores y usuarios aparecen como una necesidad de la población, desprotegida frente a un mercado agresivo al que deviene imprescindible regular a los fines de resguardar al consumidor, teniendo en cuenta que mediante el consumo se satisfacen las

necesidades humanas ^[1260]. Así, a la desigualdad natural del consumidor se propicia corregirla mediante desigualdades jurídicas, lo cual converge en la formulación del derecho del consumo como un derecho *protectorio* ^[1261], teniendo en cuenta que el derecho civil tradicional es generalmente lento en el reconocimiento de los cambios sociales ^[1262]. Este derecho protectorio consiste en contemplar esa imposibilidad cierta que aqueja al consumidor y le impide en muchos casos juzgar por sí mismo calidades, precios, materiales de elaboración, *condiciones y modalidades de contratación* ^[1263].

3.5.1.7.1. ¿Beneficios para los consumidores?

Tatiana Cutts, de la prestigiosa LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE afirma ^[1264] que son bien conocidas las ganancias de eficiencia producidas por la automatización contractual, pero también puntualiza que existen nuevos riesgos para los consumidores al utilizar estructuras contractuales que dependen de lenguajes de programación que eliminan la posibilidad de interferir en el cumplimiento del contrato. En efecto, puntualiza Cutts los riesgos asociados a ciberataques, bien ejemplificado en el caso *TheDAO* ^[1265], y sostiene que los intermediarios usuales (e.g. Amazon, Uber) normalmente absorberán el costo de cualquier ciberataque, aunque no estén obligados. Ello no ocurre en una plataforma descentralizada como *blockchain*, donde no hay sino relaciones peer-to-peer ^[1266].

También se han puntualizado ^[1267] los riesgos específicos que podrían existir por la utilización de contratos inteligentes en las operaciones de crédito para consumo ^[1268], ya que en casos de abusos:

“The immutable nature of a Smart Contract means that a court could not simply order the obligation void with any practical

effect, as is the case with an ordinary contract, because the courts are no longer the primary enforcement mechanism. This presents something of a “logistical nightmare” for a court to resolve, requiring it to somehow reverse the operation of the Smart Contract. Ideally, the Smart Contract would have a variation function to account for such contingencies which a court could use to make alterations. However, such a term would not favour Scaley (i.e. el prestamista) and therefore likely would not form part of the Smart Contract code, given that they would create it. A more complicated solution would be to order a cancelling Smart Contract going in the other direction. This would require Scaley (i.e. el prestamista) to automatically reimburse \$500 to the consumer each year as soon as it was paid. Notably, **these complex solutions show the difficulty of regulating Smart Contracts entirely through ex-post means and the issues that arise when the court is competing with a powerful digital enforcement mechanism outside of their practical jurisdiction.** A person may even commit contempt of court because the technology they used is unable to adapt to the court’s order, though this is an issue that is outside of the scope of the current paper. [\[1269\]](#)” (el resaltado es mío).

Es interesante en este punto traer a colación lo dispuesto por el Art. 83.L de la *Credit Contracts and Consumer Finance Act* de 2013 vigente en Nueva Zelanda [\[1270\]](#), recientemente modificada en 2020 para regular específicamente los mecanismos tecnológicos que permiten el recupero de bienes vendidos con financiación [\[1271\]](#), y dispone:

“83L - Use of disabling device

(1) This section applies where a consumer credit contract provides that the creditor—(a)has a security interest over **consumer goods to which a disabling device is connected**; and (b)has a right to activate the disabling device.

(2) Neither a creditor nor a creditor's agent may activate a disabling device unless— (a) there has been a **breach of the consumer credit contract** by the debtor that is sufficient, according to the terms of the contract, to give rise to the creditor's right to activate the disabling device; and

(b) the creditor or the creditor's agent **has given the debtor reasonable notice, in advance of the activation**,—(i) that the disabling device is to be activated; and (ii) about what action the debtor may take to prevent the disabling device being activated.

(3) In this section and [section 83M](#),—“activated”, in relation to a disabling device, means that the disabling function of the device has been switched on, with the result that— (a) the **debtor is prevented from using the consumer goods**; or (b) the **debtor's use of the consumer goods is limited**; or (c) the **creditor is able to locate the consumer goods**; or (d) the creditor is able to achieve any other similar outcome that is of a direct or indirect benefit to the creditor in relation to the relevant consumer credit contract; “disabling device” means a device that is attached to consumer goods, the functions of which, when activated, include 1 or more of the following: (a) preventing the consumer goods from being used: (b) limiting the debtor's use of the consumer goods: (c) enabling the creditor to locate the consumer goods: (d) achieving any other similar outcome that is of direct or indirect benefit to the creditor in relation to the relevant consumer credit contract.”

(el resaltado es mío).

Se ha sostenido que la regulación de la *Credit Contracts and Consumer Finance Act* incluye cualquier contrato inteligente que pueda ser utilizado como mecanismo de garantía del oportuno cobro por parte del proveedor de un bien –e.g., financiación prendaria– , al iniciar la desconexión remota del bien cuando la falta de pago en tiempo y forma se verifique [\[1272\]](#):

“Smart Contracts can act as a “disabling device” under the CCCFA to the extent that they prevent consumer goods from being used, limit the debtor’s use of the consumer goods, or enable the creditor to locate the goods. The electronic application linked to the car and the Smart Contract fits within this definition by preventing the car from being used when payment fails and allowing Scaley (i.e. el acreedor prendario) to locate the car via GPS.”

3.5.1.7.2. *Constitución Nacional, CCCN, ley especial y otras normas tuitivas*

En Argentina, la defensa del consumidor y del usuario tiene base constitucional en el Art. 42^[1273], con una serie de principios generales de protección mínima contenidos en el CCCN^[1274], una ley especial, la Ley N° 24.240, con ha sufrido doce modificaciones desde 1993^[1275] y muchas normas específicas que integran la tutela consumeril, e.g, ley de seguros, de entidades financieras, de transporte terrestre, de medicina prepaga, régimen de tiempo compartido, régimen de tarjeta de créditos, Ley de Defensa de la Competencia, régimen de deslealtad comercial contenido en el Decreto N° 274/2019, entre otras.

3.5.1.7.3. *Definición de consumidor o usuario. Airdrops*

Las definiciones del CCCN^[1276] y de la ley especial^[1277] sobre quién puede ser considerado consumidor permiten, sin mucho esfuerzo, incluir a los usuarios directos e indirectos^[1278] de contratos inteligentes, incluyendo a las personas jurídicas que los utilicen como consumidores finales^[1279]. Queda cubierta por el régimen tuitivo del consumo también la provisión gratuita de bienes o servicios, incluyendo regalos, con lo cual se incluirían aquí los *airdrops* de tokens digitales, que son formas de atraer usuarios

teniendo en miras una ulterior contratación onerosa [\[1280\]](#).

3.5.1.7.4. *Proveedor de contratos inteligentes, o que utiliza contratos inteligentes*

El Estatuto del Consumidor se activa cuando existe una relación de consumo entre un consumidor o usuario, por un lado, y un proveedor, por el otro. Por ende, la definición de proveedor es también central, y se encuentra en el CCCN [\[1281\]](#) y en la ley especial [\[1282\]](#), y es toda persona humana o jurídica, pública o privada, que actúa profesionalmente, aún en forma ocasional, en la comercialización de bienes o servicios. El proveedor es el experto, y el usuario es el profano.

Ahora bien, en relación a un *Smart Contract*, el proveedor puede ser tanto un programador profesional [\[1283\]](#) que ofrece específicamente servicios de programación de *Smart Contracts*, o bien un proveedor de otro tipo de bienes y servicios, que utiliza profesionalmente *Smart Contracts* como una forma innovadora de comercializarlos.

3.5.1.7.5. *Información y publicidad en materia de contratos inteligentes*

El derecho a la información es cardinal en el Estatuto del Consumidor, está también reflejado en el CCCN [\[1284\]](#) y en la ley especial [\[1285\]](#), y es realmente potente. En materia de contratos inteligentes, este derecho sin dudas se vuelve aún más potente, en función del contexto *on-chain* en el que operan los contratos inteligentes, debiéndose asumir una total carencia de información y *expertise* por parte del usuario, en razón del lenguaje de programación utilizado [\[1286\]](#).

El deber de información del proveedor lo obliga a entregar información en forma cierta y detallada, respecto de todo lo relacionado con las características esenciales de los bienes y servicios que provee, las condiciones de su comercialización y toda otra circunstancia relevante para el contrato,

antes, durante y después de la relación de consumo [\[1287\]](#) .

Evidentemente, en materia de contratación inteligente, el foco estará puesto en la información entregada *antes de iniciar un contrato inteligente*, es decir, en la etapa pre-contractual, incluyendo la publicidad. En este sentido, cabe hacer una precisión ya indicada más arriba: el proveedor puede ser tanto (i) un programador profesional –o una empresa de programación– que ofrece específicamente servicios de programación de *Smart Contracts*, o bien (ii) un proveedor *de otro tipo de bienes y servicios*, que decide utilizar profesionalmente *Smart Contracts* como una forma más de comercializarlos. En éste último caso, es previsible que el contrato inteligente sea pre-redactado en todas sus partes esenciales, y por ende, estemos frente a un contrato por adhesión, o un contrato formulario. En este caso, el art. 38 de la Ley N° 24.240 dispone:

“Contrato de adhesión. Contratos en formularios. La autoridad de aplicación vigilará que los contratos de adhesión o similares, no contengan cláusulas de las previstas en el artículo anterior. La misma atribución se ejercerá respecto de las cláusulas uniformes, generales o estandarizadas de los contratos hechos en formularios, reproducidos en serie y en general, cuando dichas cláusulas hayan sido redactadas unilateralmente por el proveedor de la cosa o servicio, sin que la contraparte tuviere posibilidades de discutir su contenido.

Todas las personas físicas o jurídicas, de naturaleza pública y privada, que presten servicios o comercialicen bienes a consumidores o usuarios mediante la celebración de contratos de adhesión, deben publicar en su sitio web un ejemplar del modelo de contrato a suscribir.

Asimismo deben entregar sin cargo y con antelación a la contratación, en sus locales comerciales, un ejemplar del modelo del contrato a suscribir a todo consumidor o usuario que así lo solicite. En dichos locales se exhibirá un cartel en lugar visible con la siguiente leyenda: “Se encuentra a su disposición un ejemplar del modelo de contrato que propone la

empresa a suscribir al momento de la contratación.” (el resaltado es mío)

Articulando la lectura del art. 38 con el art. 37^[1288] de la Ley N° 24.240, puede entonces sostenerse que un proveedor que decida utilizar contratos inteligentes como forma de comercializar otros bienes o servicios, sean éstos *off-chain* o *on-chain*, deberá previamente presentar el código de programación –código fuente– a las autoridades de aplicación del Estatuto del Consumidor en la jurisdicción de que se trate, para que éstas verifiquen que el código, en su funcionalidad testeada, no contenga cláusulas abusivas, que desnaturalicen las obligaciones del proveedor o restrinjan los derechos del usuario del contrato inteligente. Además, deberá publicar en su WebSite el código del contrato inteligente que se utilizará. La falta de cumplimiento de estas dos obligaciones, autorizarán al usuario de un contrato inteligente a demandar la nulidad del contrato.

3.5.1.7.6. Riesgos derivados del uso de contratos inteligentes en la comercialización de bienes y servicios. Facultad de revocación

Finalmente, es evidente que cuando los contratos inteligentes tengan contacto con consumidores o usuarios finales, el proveedor habrá comercializado sus bienes y servicios mediante medios electrónicos, y se tratará, innegablemente, de contratos –inteligentes– celebrados a distancia^[1289], que son, a la vez, contratos electrónicos. Se ha sostenido que la ingeniería de las implementaciones de estos contratos electrónicos es capaz de superar las habilidades informáticas medianamente desarrolladas, y hasta ciertas elevadas capacidades al respecto^[1290].

Considerar a un *Smart Contract* como un contrato celebrado a distancia producirá, en el derecho vigente, dos importantes consecuencias: (i) el proveedor debe informar al usuario, además del contenido mínimo del contrato, todos los datos necesarios para utilizar correctamente el medio elegido, para *comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos*^[1291]; y (ii) el usuario tendrá la

facultad de revocar el contrato dentro de los diez días de celebrado, siendo éste derecho irrenunciable ^[1292] y, además, es un derecho que no se extingue ni caduca en caso de no informarse sobre la posibilidad de revocar ^[1293].

Por un lado, por la redacción dada al art. 1107, CCCN, pareciera posible argumentar que el reparto de riesgos por la utilización de un *Smart Contract* puede ser materia a negociar entre el consumidor o usuario, y el proveedor. Sin embargo, parece difícil que un juez vacile en anular una cláusula de limitación de responsabilidad a favor del proveedor por mal funcionamiento de un contrato inteligente que el mismo decidió utilizar.

Por otro lado, la facultad de revocación del usuario plantea la dificultad de cómo volver atrás una transacción en una *blockchain* pública, en el caso hipotético que el consumidor o usuario se retractase. Esta posibilidad debiera ser tenida especialmente en cuenta al programar el contrato inteligente, embebiéndola directamente en el código fuente. En el caso que se utilizase una *blockchain* privada, o permissionada, quizás el problema sería de más fácil resolución.

Finalmente, para el caso que los bienes y servicios comercializados sean puramente digitales, es posible argumentar que su comercialización a través de contratos inteligentes no autorizaría al consumidor o usuario a revocar la operación, en función de una interpretación armónica del art. 1116, CCCN:

“Excepciones al derecho de revocar. Excepto pacto en contrario, el derecho de revocar no es aplicable a los siguientes contratos:

los referidos a productos confeccionados conforme a las especificaciones suministradas por el consumidor o claramente personalizados o que, por su naturaleza, no pueden ser devueltos o puedan deteriorarse con rapidez; ^[1]_[SEP]

los de suministro de grabaciones sonoras o de video, de discos y de **programas informáticos que han sido decodificados por el consumidor, así como de ficheros informáticos, suministrados por vía electrónica, susceptibles de ser**

descargados o reproducidos con carácter inmediato para su uso permanente;

los de suministro de prensa diaria, publicaciones periódicas y revistas.” (El resaltado es mío).

3.5.1.8. Blockchains, Contratos Inteligentes vs. Defensa de la Competencia. Efectos de Red vs. Efectos del Token

3.5.1.8.1. Id quod plerumque accidit

A toda (gran) innovación casi siempre le ha seguido un cambio (o, a veces, un terremoto) competitivo.

Especialmente en materia de plataformas y mercados digitales, desde que nace una innovación (e.g., *blockchain* en 2009, Facebook en 2004, AWS en 2006), va penetrando lentamente en el mercado por uso y adopción. Muchas tecnologías avanzan diariamente con pequeñas innovaciones incrementales, otras se rezagan. Mientras va madurando *con y por* el uso, toda nueva tecnología se afianza y avanza; algunas a veces se catapultan y viralizan con hallazgos exponenciales, o cuasi-exponenciales, o semi-disruptivos. Pero siempre avanzan lentamente, en tono incremental. O desaparecen.

En efecto, acéptese que la exponencialidad o cuasi-exponencialidad pocas veces se manifiestan súbitamente de un día al otro, pero desde el momento dado en que su utilidad es manifiesta –e.g. Bitcoin, 2009, Internet, 1990– comienzan a producir súbitas micro-revoluciones socio-culturales. También es cierto que, a veces, sus efectos son más intensos, como olas de un Tsunami, que cuando impactan en mercados poco eficientes, o poco competitivos, o poco innovadores, los disruptan.

Si los mercados fueran perfectos, la innovación y la competencia siempre irían de la mano, por ser el modo en que la *eficiencia* lo indica.

Pero, al contrario, lo cierto es que en los (imperfectos) mercados humanos, competencia e innovación suelen ir enfrentados, y pocas veces van bien coordinadas. Huelga decirlo, no brillan los estímulos a la competencia y a la innovación, salvo casos contados con los dedos de ambas manos. Con

carácter axiomático, puede afirmarse que sin competencia no hay necesidad de innovar. La ineficiencia se resiste a innovar, y así ha habido, por ejemplo, muchos cárteles empresarios que acuerdan precisamente no invertir en I+D, o reducir su inversión en innovación. Me viene a la mente el cártel de los pañales colombiano [\[1294\]](#). Otras veces, son las mismas *innovadoras* empresas que lideran nuevos mercados gracias a un conjunto de desarrollos tecnológicos propios, las que son permeables a abusar de su poder e intentar extenderlo a otros mercados donde no son líderes (Windows Media Player [\[1295\]](#), Google Search [\[1296\]](#)).

En otros casos, la innovación incremental no disrupta tan violentamente los mercados, sino que los obliga a aceptar un estado de *reinención permanente* bajo pena de desaparición, y lentamente, tanto la tecnología más ineficiente como su mercado de usuarios y clientes desaparece y migran de valor, respectivamente. Ejemplo de esta dinámica: caso de Kodak, BlackBerry, o el VHS.

Esa disrupción tecnológica, intensa o suave, según se vea, lector, es la que produce los frecuentes terremotos competitivos, que suelen seguir a la (gran) innovación, y en menor medida, a las innovaciones intra-tecnológicas. Adviértase que en solo 12 años, *Blockchain* --casi-- permitió disruptar el mercado financiero con los bitcoins y miles de altcoins. *Blockchain* --casi-- disrupta los sistemas tradicionales de voto [\[1297\]](#). Finalmente, probablemente el mercado financiero será disruptado por el Yuan Digital, *on-chain*, o por Libra, también *on-chain*. Son solo muestras incrementales de la innovación.

Ahora bien, para llegar a la exponencialidad, o lo que es lo mismo, a la masiva adopción de una tecnología o innovación dada, suele ser condición necesaria que una tecnología permita construir confianza *en y de* sus prestaciones, y allí, sólo allí, es cuando puede avanzar, de modo firme, hacia el estadio evolutivo posterior, dejando atrás a los audaces *early adopters*, para entrar a un estadio de uso masivo donde entran a jugar los poderosos efectos de red, tan estudiados por la Economía.

Los efectos de red en los sectores digitales indican que mientras más se

utiliza una tecnología, más interés tienen nuevos usuarios en utilizarla ^[1298]. Así, una vez que se supera una cierta masa crítica de usuarios, el valor derivado del servicio es mayor que su precio, lo que a su turno produce que se sumen más usuarios. Estos efectos de red toman un contorno particular en *blockchain*, al aparecer los *tokens* funcionales, de pago o de inversión en una plataforma, con operabilidad multi-plataformas, que funcionan como un gran incentivo que *acelera notablemente* la captación de usuarios.

Piénsese en Internet, que es –en sí misma– una red descentralizada, quizás la más grande a la fecha creada, y repárese en su desarrollo no exponencial, sino incremental desde 1990 a 2020, es decir, a lo largo de 30 años.

Piénsese en el poder de mercado que, por ejemplo, pudo detentar Microsoft con el Windows y sus *features* –especialmente los que se vendían atados–, en EE.UU durante la década del 1990-2000.

Piénsese en el efecto del Google Cloud y la lluvia de servicios digitales de la nube, que nació apenas en 2008.

Piénsese en la eficacia del modelo de economía de la suscripción de Netflix o de Spotify, que rápidamente capta cuota de mercado, pero, piénsese también, en los impactos y disrupciones que producen tales modelos de plataforma en la industria de la distribución audiovisual.

Piénsese en la cartera de clientes de AWS en 2020, en el mercado de *Infrastructure-as-a-Service*, o en los efectos económicos y competitivos de su integración vertical con un marketplace muy relevante. Repárese en los disgustos (y grandes pérdidas económicas) provocados por actos anticompetitivos de Google en el mercado de la publicidad, las reputaciones comerciales digitales y los servicios de búsqueda digital europeos.

En varios de los casos citados, se encuentra la misma relación: competencia e innovación, enfrentados.

En mi poco científica opinión, ya que no poseo más evidencia que mi propia, subjetiva, y sesgada percepción personal, pareciera que abundan los abusos anticompetitivos cuando las empresas que lideran una tecnología comienzan a usufructuar la fase de uso masivo de la misma, e.g. Internet

Explorer vs. Netscape^[1299]. Aparecen allí los abusos tecnológicos de los (nuevos) líderes de (nuevos) mercados que son, muchas veces, verdaderos océanos azules reservados para unos pocos corsarios tecnológicos. Así, es lógico señalar algunos puntos de fricción (actuales y futuros) entre la *blockchain*, los contratos inteligentes, y la defensa de la competencia. Son, como se ha dicho, los terremotos que siguen a la (gran) innovación.

En este sentido, señala Schrepel^[1300] que en la actualidad nos llama la atención la competencia entre empresas de tecnología como Google, Uber, Facebook, Amazon –todas plataformas centralizadas–, pero afirma Schrepel que, en un futuro cercano, la atención estará puesta en la competencia entre *blockchains*, y en la competencia entre plataformas descentralizadas *on-chain* vs. plataformas centralizadas *off-chain*, competencia entre tecnologías, y competencia intra-tecnología, todo al amparo de los clásicos efectos de red, combinados con los nuevos efectos del token, i.e., mucho mayor rapidez de captación de usuarios *on-chain* vis-à-vis que los típicos efectos de red *off-chain*^[1301]. Por ello afirma Schrepel:

The incentive system created on public blockchain also creates a strong inducement to join quickly, contrary to what happens on digital platforms outside of the blockchain eco-system. **Indeed, network effects are created by a critical mass**, meaning that there is a real connection between the number of users and the utility of the product or service. Therefore, when the critical mass is not reached, the interest in joining the network of existing users is low. Blockchains, however, operate differently because they are “**adding financial utility when application utility is low**” (...) “**token effects**” (...) operate somewhat **differently** than network effects. Token effects are created more easily on blockchain than network effects off blockchain because of the financial disconnect created between the incentive to join the service and its utility. **Initial Coin Offerings for instance, incentivize coin holders to make the blockchain well-known and prosperous as soon as possible.**

Other blockchains give away tokens, which is called an “**airdrop.**” When doing so, they usually impose several conditions, the most common is the creation of a user account via a social network in order to get access to the new user’s entire contact list. Here, **the incentive to join is particularly high when the value of the tokens is low. This phenomenon is not seen outside of blockchain because companies would have to give dollars and euros to attract customers, which would be prohibitively costly (...)** the intrinsic characteristics of blockchain might cause **token effects to be created even faster than network effects;** however, they may also disappear faster. [\[1302\]](#),” (los resaltados son míos).

En la competencia por los usuarios, las plataformas *on-chain* competirán con plataformas establecidas y tradicionales *off-chain*, que son, en sí mismas, *intermediarios*. En lugar de loggarse con el perfil de Facebook, en un futuro próximo te *loguearas* a una aplicación con una identidad propia, descentralizada, soberana, *Self-Sovereign Identity* [\[1303\]](#), afirma Schrepel, quien remata: [\[1304\]](#) .

“...platforms would have to find new ways to incentivize their users to give access to their data. In other words, because of blockchain, the business model of digital products and services may need to be entirely rethought in the coming years [\[1305\]](#),”

Y, cita a Vitalik Buterin, quien afirma:

“instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.” [\[1306\]](#)

3.5.1.8.2. La definición de mercados relevantes on-chain

¿Cómo definir los mercados digitales relevantes en un entorno de *blockchain*? ¿Cuáles son los productos o servicios sustitutos? ¿Hay un mercado geográfico? Se proponen muchos enfoques para responder a estos interrogantes. Probablemente, cada *blockchain* –i.e, abierta, privada– podría *per se* ser considerada un mercado relevante; o en función de su cantidad de usuarios, se podría determinar la participación de mercado de cada una; o quizás se determine el mercado en función de la funcionalidad de *Smart Contracts* –aplicaciones *on-chain*, *Daaps*, *DAOs*, *DACs*– que soportan, pudiendo diferenciarse entre *blockchains* 1.0, 2.0 y 3.0.

Así, también se podrían analizar las conductas (anti) competitivas de una aplicación puntual en *blockchain*, desde el punto de vista de los desarrolladores, de los pools de mineros y de los usuarios. ¿Son posibles los abusos de posición dominante en *blockchain*? ¿Y en una *blockchain* pública donde hay visibilidad de transacciones aunque con pseudonimia? ¿Quién puede ser considerado responsable por los actos anticompetitivos que puedan desarrollarse en la *blockchain* de Bitcoin? ¿Puede aplicarse la diferenciación de productos a cada *blockchain*, dando lugar a competencia monopolística? ¿Importa la cantidad de bloques de una *blockchain* o la extensión de su registro para considerar su posición en el mercado? ¿Puede considerarse a las *blockchains* públicas como integrantes de un mercado de servicios digitales distinto del de las *blockchains* privadas?

3.5.1.8.3. Conductas anticompetitivas unilaterales on-chain

Según Schrepel, a nivel de plataformas de *blockchain* –lo que él denomina *Layer 1* ^[1307] – es en las *blockchains* privadas donde existe mayor riesgo de abusos de posición dominante, bajo formas de negativa de venta –o de permiso de acceso ^[1308] –, ventas atadas y en paquetes ^[1309], innovación predatoria ^[1310], precios predatorios ^[1311], *margin squeeze* ^[1312], cláusulas de exclusividad ^[1313], descuentos anticompetitivos ^[1314], y abusos

explotativos de posición dominante y discriminación de precios ^[1315].

3.5.1.8.4. *Colusión mediante contratos inteligentes*

Schrepel también analiza las conductas anticompetitivas concertadas *facilitadas* por contratos inteligentes *on-chain* ^[1316]. Menudo (nuevo) desafío para todas las leyes antitrust del mundo.

En este sentido, se ha afirmado que la colusión suele aparecer cuando las famosas cinco fuerzas de Porter ^[1317] están presentes en un mercado dado, reduciendo la rentabilidad de las empresas competidoras. Así, la colusión se facilita sobremanera si hay altas barreras a la entrada, existen productos o servicios sustitutos de mala calidad, y existe poco poder negociación por parte de los consumidores o usuarios y de los proveedores ^[1318]. Afirma Schrepel que la *blockchain* facilitará ^[1319] la colusión explícita en tales mercados ^[1320] y también la tácita ^[1321]. En sus propios términos:

“blockchain can be used as a medium for these collusive agreements, or even be the subject of an agreement in itself, depending on the conditions of entry, use and exit of the technology (...) companies achieve the highest (illegal) gain when they trust each other, making it often difficult for the regulator to identify these practices. Trust tends to direct the players toward a more cooperative outcome because it pushes them to accept to being vulnerable vis-à-vis someone else, and when they cooperate effectively, detection is complicated (...) **Blockchain can play a key role in this respect by allowing more cooperation between the players.** Even more, combined with Smart Contracts, blockchain makes the colluders trust each other because the terms of the agreement are immutable. Moreover, to the extent that the technology allows for binding agreements, the need to rely on the threat of

punishmentstrategies diminishes, which make collusive outcomes more stable compared to such outcomes in noncooperative games (...) several studies estimate that the percentage of detected cartels is only between 10% and 33% in the post-World War II era, which proves that leniency procedures are not sufficient in themselves. [\[1322\]](#)” (el resaltado es mío).

Desde tal perspectiva, Schrepel no duda en afirmar que es posible la colusión *on-chain*, y que, de hecho, va a ocurrir, ya que la *blockchain* facilita tanto los acuerdos anticompetitivos con efectos ilegales *off-chain* [\[1323\]](#), como la propia colusión sobre servicios brindados *on-chain* [\[1324\]](#), dificultándose la represión de ambos tipos de acuerdos debido a la pseudonimidad imperante en entornos *on-chain* [\[1325\]](#).

En efecto, empresas que compiten *off-chain* podrían perfectamente intercambiar información comercial sensible y concertar precios, a través de *blockchains* públicas, de manera segura y encriptada. En estos casos, lo prohibido por todas las leyes antitrust del mundo es la práctica entre competidores de concertar decisiones de negocio [\[1326\]](#) –precios, cantidades, etc.–, sin importar el medio a través del cual acuerdan [\[1327\]](#). Respecto de *blockchains* privadas, la potestad de sus creadores de discrecionalmente permitir (o no) el acceso, lectura y carga de datos a favor o en contra de una o algunas de las empresas participantes, o sus distribuidoras, puede también generar efectos anticompetitivos.

En otro escenario, también puede existir riesgo anticompetitivo si grupos de usuarios de una *blockchain* se ponen de acuerdo para modificar protocolos de gobierno en un modo que les convenga.

Así, los mineros que normalmente se agrupan en pools de minería podrían decidir adoptar decisiones anticompetitivas [\[1328\]](#), incluyendo decisiones de cambio del protocolo de gobierno, para auto-favorecerse [\[1329\]](#). Los

desarrolladores, por su parte, son pequeños grupos con enorme poder en una *blockchain*, y como tal, pueden intentar celebrar acuerdos anticompetitivos para auto-favorecerse [\[1330\]](#). Finalmente, los usuarios de ciertas *blockchains* pueden tener derechos de voto, donde un grupo limitado de usuarios posee una cantidad significativa de tokens, y pueden, en consecuencia, adoptar decisiones anticompetitivas para auto-favorecerse [\[1331\]](#).

Por otro lado, los contratos inteligentes desplegados sobre *blockchain* también pueden ser utilizados para violar leyes de defensa de la competencia [\[1332\]](#) y garantizar el cumplimiento de un cartel [\[1333\]](#).

3.5.1.8.5. Cinco principios esenciales que deben ser tenidos en cuenta al regular la blockchain

Finalmente, señala Schrepel que la regulación que se pretenda implementar sobre el entorno *on-chain*, no debiera afectar cinco principios que son fundacionales en esta tecnología.

3.5.1.8.5.1. Pseudonimidad como característica esencial

Afirma Schrepel que cualquier regulación sobre y del entorno *on-chain*, debe partir de reconocer a la pseudonimidad:

“as essential to the blockchain, since imposing upstream regulations that mandate disclosure of users’ identities would be contrary to the very essence of blockchain technology and will actually eliminate an alternative model to most of the technologies in use today where users’ real-life identify is known and monetized by companies. Of course, pseudonymity does not come without its challenges; however, the concept remains core to blockchain’s existence. [\[1334\]](#)”

3.5.1.8.5.2. *Arquitectura distribuida*

Toda regulación que se diseñe debe también reconocer la naturaleza de la arquitectura distribuida de la *blockchain*:

“This core principle of blockchain creates distributed power, meaning that no central point of failure exists and the harm from one person’s reckless behavior is contained solely to that person. [\[1335\]](#),”

3.5.1.8.5.3. *Transmisión peer-to-peer entre usuarios*

El tercer principio fundamental de las *blockchains* es la transmisión peer-to-peer de información y valor entre usuarios:

“The existence of a transmission system, which is vital to the use of blockchain, must not be challenged by regulations. Doing so would amount to reintroducing middle-market companies into the blockchain ecosystem, artificially and unnecessarily making blockchain less attractive. [\[1336\]](#),”

3.5.1.8.5.4. *Protocolos de consenso*

El cuarto principio fundamental del entorno *on-chain* son los protocolos de consenso:

“Creators must remain free to choose the consensus mechanism they wish to use. Therefore, blockchain users should be free to participate in the block validation process they deem best without becoming liable for assenting to an anticompetitive practice the blockchain may be involved with

at another time. [\[1337\]](#)”

3.5.1.8.5.5. *Inmutabilidad*

El quinto principio fundacional de la *blockchain* es su carácter inmutable. Admitir que una entidad pueda borrar datos, o detener las transacciones que ocurren en una *blockchain*, afectaría gravemente la confianza en el sistema, uno de sus atributos más importantes [\[1338\]](#). Sin embargo, desde su propio diseño, las *blockchains* podrían permitir que:

“to embed regulatory measures into the blockchain’s governance. Just as the mechanism by which users would vote to reveal the identity of an individual involved in anti-competitive practices on a private blockchain, a mechanism could be developed in which blockchain users vote on the creation of forks, determined by courts or antitrust agencies, in order to delete or stop transactions. Blockchain communities agreeing to introduce such mechanisms would be treated by regulators and courts as being more in line with the law than blockchains refusing to do so. Stricter measures challenging one of the five principles could be imposed on the latter, which could be a powerful tool at the disposal of public authorities.

The introduction of such voting mechanisms would be binding when used to determine whether an individual’s identity should be disclosed, whether to put an end to certain transactions, whether a ban on “layer 2” applications should be instituted, or whether there should be interference with a key aspect of a blockchain’s function. One may also consider the possibility that public authorities could mandate the presence of voting into blockchains without the need to ask for any permission, or even going further, to force the creation of hard forks. Time will show which mechanisms will be appropriate in

specific situations [\[1339\]](#).”

Concluye Schrepel afirmando, en opinión que comparto plenamente:

“Regulations that challenge one of these five principles could cause blockchain to lose its utility. The way blockchain will evolve is uncertain, and choices made by blockchain communities will fundamentally affect what values are built into it as well as the outcome users and society can gain from it. For this reason, it is tempting for regulators to get involved in how blockchain will turn out. But the question is “whether we’re capable of making those choices,” knowing that **“law tends to arrive at basic answers before the right questions have been asked.”** The issues are too fundamental not to let blockchain transformations emerge on their own thanks to its millions of users. Regulatory humility in light of these bedrock blockchain principles will ensure that the blockchain continues to develop to its full potential [\[1340\]](#) (...) Self-regulation and co-regulation should also be considered as serious alternatives [\[1341\]](#).” (el resaltado es mío)

3.5.1.9. Contratos Inteligentes vs. Régimen Falencial

En este apartado se analizarán las fricciones que los contratos inteligentes pueden producir al tomar contacto con el régimen falencial. Primero se esbozarán muy resumidamente algunas notas salientes del régimen falencial argentino, y luego se pondrá foco en aquellos institutos falenciales que representan desafíos para los desarrolladores y usuarios de *Smart Contracts*.

3.5.1.9.1. El Derecho Concursal. Principios. Procesos. Cesación de pagos

El Derecho Concursal es definido como un conjunto de principios y

normas destinado a regular una realidad indeseada: la impotencia patrimonial que afecta a una persona, humana o jurídica, para pagar sus deudas de manera regular ^[1342], y que adquiere un lógico protagonismo en los períodos de crisis macroeconómicas. En Argentina, el régimen falencial está contenido principalmente en la Ley de Concursos y Quiebras N° 24.522 (LCQ) ^[1343].

Los principios que rigen los institutos concursales son la universalidad, reflejado en los arts. 1, 107 y 108 LCQ ^[1344], la colectividad de acreedores reflejado en los arts. LCQ 21 y 132 ^[1345], la concurrencia de acreedores y su igualdad, regladas en los art. 32, 16, 43, 56, 87, 122, y 118 LCQ ^[1346], la oficiosidad fijada en el art. 274 y también en el art. 36 LCQ ^[1347], la inquisitoriedad dispuesta en el art. 274 LCQ ^[1348], la unidad que fluye de los arts. 202 y 239, LCQ ^[1349] y la conservación de la empresa que irriga toda la LCQ ^[1350].

El régimen falencial argentino regula dos procesos falenciales: el concurso preventivo y la quiebra ^[1351]. El concurso supone un acuerdo *preventivo* entre el deudor y sus acreedores, que reglará el cumplimiento de las obligaciones pendientes que generaron su insolvencia. Se pactan usualmente nuevos plazos, intereses, quitas y esperas, incluso asociarse con los acreedores, capitalizándose sus créditos. Dicho acuerdo requiere que una doble mayoría de acreedores con derecho a voto –por personas y por capital– lo apruebe, para volverse obligatorio, incluso para los que no los aceptaron o estuvieron ausentes. Sin esa doble aprobación, el deudor será declarado en quiebra indirecta, salvo casos de salvataje ^[1352].

La quiebra, a su turno, es la ejecución del patrimonio insolvente, previo desapoderamiento, con el fin de repartir el producido entre los acreedores de acuerdo a sus privilegios ^[1353]. Ambos procesos requieren la cesación de

pagos ^[1354] como presupuesto objetivo de apertura de un proceso universal. En ambos procesos, interviene el síndico y otros funcionarios cuyas funciones son indelegables ^[1355].

3.5.1.9.2. Efectos del concurso preventivo y la quiebra

El dictado de la sentencia de apertura del concurso preventivo produce importantes efectos jurídicos ^[1356] sobre las relaciones jurídicas de título o causa *anterior* a la presentación en concurso:

- i) régimen especial de administración del patrimonio del deudor bajo vigilancia del síndico (arts. 15, 16 y 17, LQC) ^[1357];
- ii) la suspensión de intereses ^[1358] en el art. 19 LCQ;
- iii) la conversión de deudas no dinerarias y en moneda extranjera ^[1359];
- iv) la compensación de créditos ^[1360];
- v) la caducidad (o no) de plazos ^[1361];
- vi) se suspende el derecho de retención ^[1362];
- vii) se tornan aplicables las reglas para los contratos con prestaciones recíprocas pendientes fijadas en el art. 20 LCQ, las reglas para algunos contratos en particular y la facultad resolutoria general, que se analizan *infra*;
- viii) el pronto pago laboral del art. 16 LCQ ^[1363]; y
- ix) una serie de efectos imperativos, procesales y personales, reglados en los arts. 21, 22, 23 y 24 LCQ entre los que se destacan el fuero de atracción, la suspensión de los juicios en trámite, la prohibición de iniciar nuevos juicios y ciertos efectos sobre las medidas cautelares ^[1364]

3.5.1.9.3. Contratos con prestaciones recíprocas pendientes, facultad resolutoria y reglas para algunos contratos en particular

La apertura del concurso impacta sobre ciertos contratos celebrados por el concursado previo a su presentación concursal. Así, el art. 20 LCQ ^[1365] fija reglas y excepciones en el concurso, y el art. 143 hace lo propio para la quiebra, aunque en términos más amplios al cubrir todos los contratos en curso de ejecución, sin distinciones, y con la mira puesta en la liquidación.

Por regla de orden público, el concurso preventivo no provoca *per se* resoluciones contractuales y el concursado podrá continuar los contratos que considere convenientes para el desarrollo de su actividad ^[1366]. El art. 20 LCQ no se aplica a contratos en los cuales el concursado ya cumplió la totalidad de sus obligaciones, o a aquéllos en los que el contratante *in bonis* ya lo hizo. Los contratos comprendidos serán aquellos en curso de ejecución ^[1367] o que, al momento de la presentación en concurso, tienen *prestaciones recíprocas pendientes*.

Respecto de los contratos comprendidos en el art. 20 LCQ, el concursado puede solicitar judicialmente su continuación ^[1368], lo que en alguna medida implica modificar la situación de un acreedor pre-concursal puntual, y también es una excepción a la carga verifcatoria respecto del cocontratante *in bonis* ^[1369]. La razón: la continuación del contrato supone un beneficio patrimonial para el concursado, e incrementa la garantía común de sus acreedores. El cocontratante obligado a continuar un contrato con un concursado tiene ciertos beneficios ^[1370], y puede decidir resolver el contrato si no se le notifica la decisión judicial de continuarlo en el plazo legal.

En la quiebra, en cambio, el art. 145 LCQ dispone la inaplicabilidad de la facultad resolutoria, legal o contractual, a partir de la sentencia de quiebra, salvo si la resolución del contrato operó extrajudicialmente o se demandó judicialmente *antes* de la sentencia de quiebra ^[1371]. La doctrina interpreta que en el concurso, si el cocontratante *in bonis* resolvió el contrato *antes* de la

presentación del concurso, tal resolución se rige por el derecho común [\[1372\]](#). Abierto el concurso, el cocontratante ya no podrá resolver el contrato por incumplimiento si se aplicara el art. 20 LCQ a su respecto.

Ahora bien, si existen incumplimientos del concursado *posteriores* a la presentación en concurso, luego de haberse decidido judicialmente continuar el contrato de que se trate, cualquiera de las partes puede resolver el contrato de acuerdo al derecho común [\[1373\]](#).

Finalmente, existen también reglas específicas para ciertos contratos: boletos de compraventa inmobiliaria [\[1374\]](#), locación [\[1375\]](#), leasing [\[1376\]](#), agencia, franquicia y concesión [\[1377\]](#), cesión de derechos [\[1378\]](#), contratos asociativos [\[1379\]](#), y para la cuenta corriente bancaria [\[1380\]](#).

3.5.1.9.4. Quiebra y desapoderamiento. Activos intangibles en el régimen falencial

Ahora bien, si el concurso como mecanismo reestructurador de pasivos no funcionó –o ante el propio pedido del deudor–, devendrá la quiebra del deudor por sentencia judicial [\[1381\]](#). Uno de sus efectos es el desapoderamiento de pleno derecho de todos los bienes del deudor [\[1382\]](#), salvo excepciones; otro efecto es la prohibición de hacer pagos al fallido [\[1383\]](#), y también se dispone la interceptación de la correspondencia del fallido [\[1384\]](#). Los bienes del fallido, incluyendo documentos y papeles, deben ser inventariados para ser liquidados [\[1385\]](#).

Sin dudas, el desapoderamiento es el principal efecto de la quiebra, es inmediato desde dictada la sentencia de quiebra y se materializa en la incautación de bienes [\[1386\]](#). El fallido sigue siendo dueño, pero no puede disponer de sus bienes [\[1387\]](#) ni administrarlos, quedando a cargo del síndico.

Los bienes sujetos a desapoderamiento son tanto materiales como

inmateriales, susceptibles de tener valor pecuniario, salvo algunos bienes excluidos [\[1388\]](#), y el fallido no podrá realizar ni recibir pagos en virtud de los arts. 107, 109 y 110 LCQ, los que serán ineficaces de pleno derecho [\[1389\]](#).

Finalmente, es habitual que en el activo falencial se encuentren derechos intangibles, como una marca [\[1390\]](#) y que la quiebra afecte relaciones patrimoniales no contempladas expresamente. En éste caso, el art. 159 LCQ dispone:

“Casos no contemplados: reglas. En las relaciones patrimoniales no contempladas expresamente, el juez debe decidir aplicando las normas de las que sean análogas, atendiendo a la debida protección del crédito, la integridad del patrimonio del deudor y de su empresa, el estado de concurso y el interés general.”

3.5.1.9.5. Acciones de recomposición patrimonial

La recomposición del patrimonio del fallido es una finalidad esencial del proceso de quiebra, y por ello la LCQ regula tres herramientas que permiten robustecer la garantía de cobro de los acreedores del fallido [\[1391\]](#), que se suman a herramientas extra-concursales contenidas en otras leyes: (i) la acción de inoponibilidad concursal, (ii) la extensión de quiebra, y (iii) las acciones de responsabilidad. Sólo se darán aquí *brevitatis causae* algunas precisiones sobre la inoponibilidad concursal, ya que pueden tener relevancia en conexión con eventuales contratos inteligentes celebrados por el fallido.

Así, la inoponibilidad concursal resguarda la *par conditio creditorum*, y permite revisar actos pasados [\[1392\]](#) del fallido celebrados dentro del período de sospecha, cuando ya se encontraba afectado por la cesión de pagos [\[1393\]](#), si produjo perjuicio a la masa [\[1394\]](#). La inoponibilidad puede tener lugar de

pleno derecho, de oficio por el juez [\[1395\]](#), o por el conocimiento que el tercero tuvo acerca del estado falencial de su cocontratante [\[1396\]](#).

Con este panorama y estas herramientas de recomposición en la LCQ, Usandizaga [\[1397\]](#) plantea una situación interesante: ¿qué sucedería cuando el fallido celebra un contrato con un tercero, mediante el cual se entregaron prestaciones equivalentes –y yo aquí agregó, sólo a los fines del debate: intercambio de moneda convencional por criptoactivos, donde el tercero es un *Exchange*– pero con la particularidad de que la prestación cumplida por el cocontratante resulta fácilmente ocultable a los acreedores –e.g. cinco bitcoins–? La doctrina mayoritaria de los concursualistas –señala Usandizaga– considera que “*si es real que al patrimonio del fallido ingresó una contraprestación dineraria equivalente al bien que este transfirió, el acto es inatacable: el tercero no es responsable por lo que el deudor hizo con el dinero recibido*” –yo agregó: lo que el fallido hizo con la llave privada que le permite disponer de los bitcoins.

3.5.1.9.6. *Smart Contracs vs. LCQ*

Vistos a vuelo de pájaro algunos los rasgos propios del régimen falencial, los contrastaremos con la nueva realidad jurídico-digital de los criptoactivos y los contratos inteligentes, siguiendo la exposición de Renato Mangano [\[1398\]](#), quien analiza tres cuestiones: (i) ¿Cómo hacer para que los criptoactivos del deudor se incorporen a la garantía patrimonial a favor de sus acreedores? (ii) ¿Cómo efectivizar las reglas de recomposición patrimonial cuando existen criptoactivos? (iii) ¿Cómo revertir transacciones de criptactivos en fraude a los acreedores?

En relación a la primera cuestión, afirma Mangano que en caso de quiebra, el síndico debe inventariar el activo del fallido, compuesto tanto por activos físicos como intangibles, incluyendo criptactivos [\[1399\]](#). Señala Mangano que, positivamente, las *blockchains* registran inalterablemente todas las transacciones, incluyendo la fecha de su adquisición, y esto tiene evidente relevancia en hipótesis falencial. Negativamente, estos criptoactivos dependen

de llaves digitales –una pública y una privada–, que no necesariamente pueden ser asociadas al fallido, quien puede voluntariamente decidir no divulgar su existencia, en perjuicio de sus acreedores, y sin que el síndico siquiera pueda enterarse. Ahora bien, si el síndico toma conocimiento de la existencia de los criptoactivos, ¿qué puede hacer para incautarlos?

En relación a la segunda cuestión, Mangano afirma que si bien el síndico cuenta con herramientas legales para recomponer el activo del fallido, al enfrentar dichas herramientas a los criptoactivos, el régimen falencial cruje por todos lados [\[1400\]](#), ya que el síndico puede ni enterarse de la existencia de dichos activos digitales. Pero aún si el síndico llegara a tener conocimiento, y el fallido hubiera dispuesto de los criptoactivos en infracción al régimen falencial, descubrirá entonces la sindicatura: (i) el carácter irreversible de las transacciones *on-chain*; y (ii) la posible pseudonimia del adquirente, i.e., la imposibilidad de descubrir su identidad real, y por ende, no tener a quién demandar [\[1401\]](#).

En relación a la tercera cuestión, Mangano sostiene que las dificultades que encontraría la sindicatura para revertir transacciones fraudulentas del fallido con criptoactivos son enormes [\[1402\]](#).

Evidentemente, compartimos con Mangano [\[1403\]](#) que el régimen falencial no está preparado para recibir a los criptoactivos, ni mucho menos a los contratos inteligentes que se desarrollarán paralelamente.

En este sentido, se ha sostenido que los contratos inteligentes podrían, de hecho, no cumplir las reglas del régimen falencial [\[1404\]](#), específicamente aquellas que la quiebra produce en las relaciones jurídicas preexistentes [\[1405\]](#). Vale traer a colación un caso que, si bien no involucró *Smart Contracts*, tiene una plataforma fáctica que luce adecuada para los casos que vendrán:

“In re **Hampton**, the U.S. Bankruptcy Court for the Eastern District of Arkansas was tasked with determining whether the

use of a manually operated GPS/SID violated the automatic stay. In this case, the debtor was required to obtain and input a special code into the GPS/SID each month for her vehicle to remain operable. The lienholder would only provide the debtor with the appropriate codes after receipt of each monthly payment. However, after the debtor filed for chapter 13, she was unable to rely on the use of her vehicle. Moreover, the debtor alleged that the lienholder, among other things, failed to provide her with the appropriate monthly codes and occasionally (and perhaps inadvertently) provided the debtor with the wrong codes. The Hampton court found that the GPS/SID “**resulted in an overt exercise of control over estate property in violation of the automatic stay.**” However, the court primarily focused its analysis on whether the “violation was willful due to the creditor’s failure to take the necessary action, such as removing the device or ensuring that [the] Debtor always had a correct code to start her car.” Although the court was unable to find any reported bankruptcy cases involving GPS/SIDs, it noted that “there are many examples of creditors exercising control over estate property by failing to take appropriate action to ensure that they did not violate the automatic stay.” The court found that while the existence of the GPS/SID was not in itself a stay violation, the creditor’s “inaction in making sure that [the] Debtor had use of her car while in bankruptcy ... caused the automatic stay to be violated.” Thus, under the Hampton analysis, **a court may impose stay-violation damages on a party to a Smart Contract who fails to take appropriate actions to ensure that the Smart Contract does not violate the automatic stay.** [\[1406\]](#)” (los resaltados son míos).

Las dificultades reseñadas llevan a la inexorable conclusión de que la programación de los *Smart Contracts* debe, de algún modo, “tener en cuenta al régimen falencial”. En este sentido, Aaron Wright, abogado especializado

en *blockchain* y co-fundador de OpenLaw, afirma que los contratos inteligentes deberán ser programados *ab initio* para transitar ciclos normales de la vida de un contrato, incluyendo la necesidad de suspenderlos o terminarlos en caso de quiebra de alguna de las partes involucradas. Así, afirma que:

“at the heart of the American bankruptcy system is the concept of an “automatic stay” provided by Section 362 of the Bankruptcy Code. Under Section 362, effective immediately upon the commencement of a debtor’s bankruptcy case, the automatic stay prohibits a wide range of actions affecting a debtor’s estate, including barring the transfer of the debtor’s actions via existing contracts. To comply with this law, **parties will need to be able to halt a Smart Contract’s execution.** Parties relying on Smart Contracts will undoubtedly run into disputes or instances where they want to halt or stop the transfer of assets, necessitating tools that grant them the ability to control the autonomy of Smart Contracts. [\[1407\]](#)” (el resaltado es mío)

Así, el protocolo de contratos inteligentes de la plataforma de *Smart Contracts* de OpenLaw, que corre en Ethereum, tiene embebida una funcionalidad que permite a las partes detener el contrato en ciertas circunstancias, apretando un botón [\[1408\]](#).

3.5.1.10. Contratos Inteligentes vs. Régimen de Protección de Datos Personales

Finalmente, es importante analizar cómo se integrarían los contratos inteligentes a la legislación nacional de protección de datos personales contenida en la Leyes N° 25.326 [\[1409\]](#), 27.275 [\[1410\]](#), 27.483 [\[1411\]](#) y en distintas Resoluciones dictadas por la autoridad de aplicación del

régimen ^[1412], principalmente, la Resolución 4/2019 ^[1413].

En este sentido, la doctrina nacional ^[1414] ha afirmado que la República Argentina va en camino a una armonización de normativa y estándares con la Unión Europea, y que ésta considera a la Argentina como un país con una protección adecuada de datos personales.

Antes de analizar la Directiva Europea de Protección de Datos, GDPR ^[1415] por sus siglas en inglés, se remarcarán los puntos en los cuales los contratos inteligentes que corren en la *blockchain* deberán probablemente ser armonizados ^[1416] con nuestra legislación sobre protección de datos (o, a la inversa, nuestra legislación sobre protección de datos ser armonizada con la inmutabilidad de la *blockchain*).

3.5.1.10.1. *Derecho al olvido: ¿Un derecho a borrar?*

El estudio del llamado *derecho al olvido* debe iniciar con el estudio del *habeas data* ^[1417], conceptualizado como una nueva institución jurídica para poder lograr efectivamente, en un Estado de Derecho, la *protección, seguridad, exactitud o rectificación, preservación o destrucción justificadas* del secreto o privacidad sobre los datos del ciudadano, que el Estado u otros entes públicos o privados tengan sobre ellos con el propósito del conocimiento y difusión permitidos de los mismos, ya sea que estén archivados o guardados en medios electrónicos o similares, porque ellos constituyen testimonios o proyecciones de la persona, de la vida, de la identidad, pensamiento cultural o instrucción, actividades sociales, económicas, religiosas, así como los de la genética, salud, orientación sexual, pensamiento político, sea que ya se hallen registrados o por registrarse, según el amparo y protección que la Constitución y las Leyes respectivas ordenen ^[1418].

En cuanto a su finalidad, se ha afirmado que busca impedir que la información contenida en bancos o registros de datos, respecto de la persona titular del derecho que interpone la acción, sea recopilada cuando está referida a aspectos de su personalidad y directamente vinculados con su

intimidad y privacidad y a que no puedan encontrarse a disposición del público o ser utilizados en su perjuicio por órganos públicos o entes privados [\[1419\]](#) .

El cuanto al fundamento del *habeas data*, se lo ha encontrado en el derecho a la intimidad como género que caracteriza la defensa de la privacidad, del honor, la imagen, la reputación, la identidad, entre otros [\[1420\]](#) .

La Ley N° 25.326 fue dictada en el año 2000 para reglamentar este derecho, y la jurisprudencia de la Corte Suprema de la Nación fue delineando el llamado derecho al olvido en los fallos *Catania* [\[1421\]](#) y *Napoli* [\[1422\]](#) , en función de lo previsto en los arts. 16 y 26 abajo transcriptos:

“Art. 16 Derecho de rectificación, actualización o supresión.

1. Toda persona tiene derecho a que sean rectificadas, actualizadas y, cuando corresponda, **suprimidos o sometidos a confidencialidad** los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. **El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión** o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de *habeas data* prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos **debe notificar la rectificación o supresión al cesionario** dentro del quinto día hábil de efectuado el tratamiento del dato.

5. **La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.**

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.” Los resaltados son míos.

“Art. 26. — Prestación de servicios de información crediticia.

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. **Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años.** Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.” (el resaltado me

pertenece).

Los últimos 20 años de doctrina y jurisprudencia argentinas han ido definiendo un *derecho al olvido* que, si bien no está explícitamente legislado [\[1423\]](#), se asume como el principio a tenor del cual ciertas informaciones deben ser eliminadas de los archivos trascurrido un determinado espacio de tiempo, desde el momento en que acaeció el hecho al que se refieren, para evitar que el individuo quede “prisionero de su pasado. [\[1424\]](#)„

En Europa, por su parte, los debates han sido también muy candentes previo al dictado de la GDPR. En efecto, en el célebre caso *Costeja* [\[1425\]](#), el Tribunal de Justicia de la Unión Europea condenó a Google –y en general a todos los intermediarios en Internet– a cumplir con el derecho al olvido vigente en Europa. Un caso reciente del año 2020 fallado en Argentina se ha hecho eco del caso *Costeja*, y ha reconocido expresamente el derecho al olvido [\[1426\]](#).

Finalmente, el proyecto de nueva ley de datos personales [\[1427\]](#) también regula el asunto, en su art. 31:

“Derecho de supresión. El titular de los datos tiene derecho a solicitar la supresión de sus datos personales de las bases de datos del responsable del tratamiento cuando el tratamiento no tenga un fin público, a fin de que los datos ya no estén en su posesión y dejen de ser tratados por este último.

La supresión procede cuando:

Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados;

El titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico;

El titular de los datos haya ejercido su derecho de oposición conforme al artículo 30, y no prevalezcan otros motivos

legítimos para el tratamiento de sus datos;
Los datos personales hayan sido tratados ilícitamente;
Los datos personales deban suprimirse para el cumplimiento de una obligación legal.
La supresión **no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, prevalezcan razones de interés público para el tratamiento de datos cuestionado, o los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables** o, en su caso, en las contractuales entre el responsable o encargado del tratamiento y el titular de los datos.
La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.” (el resaltado es mío).

En el mensaje de elevación de la norma proyectada, se señala que el derecho al olvido *“ha traído muchas discusiones teóricas y críticas sobre su aplicación en la práctica, dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información. De allí que en la propuesta que se somete a consideración, si bien se reconoce este derecho, se ha aclarado especialmente que el derecho de supresión no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.”*^[1428]

3.5.1.10.2. Decisiones basadas únicamente en el tratamiento automatizado de datos

Otra cuestión que probablemente generará discusión en conexión con los contratos inteligentes, es lo dispuesto en la citada Resolución 4/2019^[1429], que contiene los llamados criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley de Protección de Datos Personales N° 25.326. Uno de dichos criterios es el siguiente:

“Criterio 2. Tratamiento automatizado de datos

En caso que el responsable de la base de datos tome decisiones basadas **únicamente** en el tratamiento automatizado de datos que le produzcan al titular de los datos **efectos jurídicos perniciosos o lo afecten significativamente de forma negativa**, el titular de los datos tendrá derecho a solicitar al responsable de la base de datos una **explicación sobre la lógica aplicada en aquella decisión**, de conformidad con el art. 15, inciso 1 de la Ley N° 25.326.” (el resaltado es mío).

Retenga, por ahora, el lector la necesidad de *poder explicar la lógica de una decisión basada en datos*, y el consecuente derecho del titular de los datos a exigir que tal explicación le sea brindada. Se volverá sobre esto *infra* en § 3.5.1.10.4.

3.5.1.10.3. General Data Protection Regulation

La Directiva Europea de Protección de Datos, conocida mundialmente como *GDPR*^[1430] entró en vigor en 2016 y tiene plena aplicación comunitaria desde el 25 de Mayo de 2018. Pensada para regular bases de datos centralizadas, la *GDPR* plantea importantes interrogantes cuando esos datos están descentralizados en una red que, como se ha visto, no es fácilmente modificable^[1431]. De hecho, al menos en materia de *blockchains* públicas, se ha afirmado que pareciera haber una incompatibilidad total con la *GDPR*, ya que los datos encriptados o hashados siguen siendo datos personales según la *GDPR*^[1432]. Existe aparentemente un conflicto entre un derecho fundamental a la protección de los datos personales, por un lado, y otro derecho fundamental, a emprender e innovar, por el otro.

En este sentido, Michèle Fink afirma con mucha razón que:

“Blockchains offer a record-keeping function that dispenses

from the need for third-party intermediation and by analogy can decentralise the collection, storage and processing of data. **This stands in sharp contrast with the current data economy, characterised by economic centralisation in the form of ‘platform power’.** Large intermediaries such as Google, Amazon, Apple and Facebook control how we search, shop and connect. **They autonomously collect, store, process and monetise our data trails.** This, in turn, enables them to expand their position of power in building on the data mountains they sit on, for instance to **train new algorithms.** Such market power has caused concern from a competition policy perspective as it burdens market entry (...) blockchains offer the promise of the decentralised handling of data and **data sovereignty**, a concept that focuses on giving individuals control over their personal data and allowing them to share such information only with trusted parties. **The GDPR shares the data sovereignty objective as it aims to give natural persons ‘control over their own personal data’.** The right to data portability in Article 20 GDPR enshrines this objective in allowing a data subject to receive data from a controller in order to give it to another controller. The **right to data portability** is an emergent concept in EU law, the contours of which remain largely undefined. There is no doubt, however, that it seeks to give data subjects more control over personal data.”^[1433] (el resaltado es mío).

En este sentido, se ha afirmado que el diseño de las arquitecturas de *blockchains* debe tener en vistas los objetivos de la *GDPR*, puesto que habría, posiblemente, un punto de unión –*meeting of the minds*– en el consagrado derecho europeo a la soberanía de los datos y a su portabilidad^[1434].

3.5.1.10.3.1. Alcance de la GDPR

La GDPR se aplica a todo dato personal de personas humanas identificables que esté archivada en registros, automatizados o no ^[1435], incluyendo las llaves públicas ^[1436] *on-chain*. Hay técnicas que permiten que los datos almacenados en cadenas de bloques puedan ser relacionados a una persona humana identificable, e.g., cruzando números IP, con identidades digitales, con datos financieros, con reputaciones digitales, con e-mails y chats en foros de tecnología, etc., salvo que sean *anonimizados* de un modo irreversible que evite su identificación. Cuando los datos son encriptados, pueden ser siempre descryptados con la llave privada *respectiva*, por lo que no es un proceso irreversible ^[1437]:

“Encryption is considered a pseudonymisation technique under the EU data protection regime given that the data subject can still be indirectly identified so that it can, on its own, not be considered as an anonymisation technique. The conclusion that transactional data that has been encrypted remains personal data for the purposes of the GDPR is accordingly unavoidable. Transactional data that has been subject to a hashing process also qualifies as personal data under the GDPR (...) hashing constitutes a technique of pseudonymisation, not anonymisation as it is still possible to link the dataset with the data subject. We thus conclude that transactional data that is encrypted or has undergone a hashing process will still be considered personal data for the purposes of the GDPR.”

3.5.1.10.3.2. GDPR vs. Blockchains: derecho a rectificar los datos y derecho al olvido

Señala Fink que el derecho a rectificar la información alojada en una *blockchain*, explícitamente consagrado en la GDPR, encuentra las siguientes limitaciones fácticas y técnicas: (i) ¿cómo identificar a todos los nodos de una *blockchain*?; (ii) aún identificados, los nodos no pueden modificar los datos almacenados encriptados *on-chain* ^[1438]. Pero, sin dudas, el mayor de los

problemas lo genera el derecho al olvido, consagrado en el art. 17 de la GDPR [\[1439\]](#). Así, afirma Fink:

“Immutability is one of blockchains’ most heralded (although exaggerated) features. They are, by definition, unable to forget as they were specifically designed to be censorship-resistant. A straightforward application of the right to be forgotten to DLTs can be excluded.”

Ahora bien, también puntualiza Fink que la ley alemana que transpoló la GDPR expresamente dispuso que el derecho al olvido puede no ser aplicable cuando la tecnología utilizada para almacenarlo no permite suprimir información [\[1440\]](#).

3.5.1.10.4. Smart Contracts, derecho al olvido, decisiones basadas en datos, y otra tecnología en ascenso: Enter the Machine Learning (una disgresión)

Habiéndose revisado los puntos más críticos vinculados a la protección de datos personales y su interacción con las cadenas de bloques, puede, *a priori*, concluirse que la utilización de contratos inteligentes en la República Argentina provocará que:

i) al seguirse los criterios europeos de alta protección de datos personales, se re-editarán aquí las mismas discusiones que giran en torno al carácter inmutable de la cadena de bloques;

ii) los contratos inteligentes tendrán acceso a datos que pueden ser considerados personales, incluyendo las llaves públicas, y en algunos casos, incluso datos sensibles;

iii) dependerá del diseño de cada cadena de bloques –públicas o privadas– la forma de implementar las medidas de resguardo de los datos personales, en atención a la inmutabilidad del registro *on-chain*;

iv) al derecho del titular del dato a exigir la supresión de datos almacenados

en una *blockchain* en virtud de un contrato inteligente, podría oponérsele la excepción proyectada en el Art. 31 –i.e. la supresión podría causar perjuicios a intereses legítimos de otros usuarios de la *blockchain*;

v) cuando el contrato inteligente tome *decisiones automáticas basadas* en datos –lo que ocurrirá siempre, en todos los casos, por su propia naturaleza computacional–, el titular tendrá derecho a recibir una explicación sobre la lógica de la decisión del contrato inteligente, lo que esperablemente habrá sido adecuadamente informado antes de iniciar el contrato inteligente de que se trate.

Ahora bien, es conveniente –y hasta necesario– hacer una digresión [\[1441\]](#) en este preciso punto de este Manual dedicado al *blockchain* y a los contratos inteligentes, y dar algunas nociones aproximatorias sobre la *Inteligencia Artificial* (IA, o *AI*, en inglés) y el Aprendizaje Automático o *Machine Learning* (ML).

3.5.1.10.4.1. Algunas precisiones en cuanto al uso de los términos

El punto de partida: la digitalización produce datos, en grandes cantidades. Esos datos sirven para entrenar algoritmos. Repárese que durante 2016 se creó la misma cantidad de datos que durante toda la humanidad, y el 90% de toda la *información digital* se ha creado entre los años 2016 y 2018 [\[1442\]](#). Teniendo en cuenta el *boom* de los datos, pero antes de dar una somera descripción de cómo funciona el *aprendizaje automático*, son necesarias algunas precisiones terminológicas.

En efecto, la llamada disciplina del *Business Analytics* es sinónimo del *Machine Learning*: se analizan datos en grandes cantidades, para extraer información y conocimiento. El BA o el ML no son más que la exploración organizada e iterativa de datos generados por una organización, pública o privada o mixta. Esta información permite tomar decisiones *data-driven*, basadas en datos, de modo de *complementar* a los expertos humanos que, hasta el momento, vienen decidiendo en exclusiva.

Otro término que suele aparecer en este ámbito es el *Business Intelligence* (BI), que tiene que ver con *visualización y monitoreo* de datos, es decir, mucho menos valor agregado que el Business Analytics. Esta *revolución* creada por el BA-ML es ahora posible por la gran cantidad de datos, más la (nueva) capacidad computacional para poder procesarlos. De allí que se diga, vulgarmente, que los datos son el nuevo petróleo, y que las refinarias son el ML y la AI. Ello así, ya que grandes cantidades de datos, tratados con ML, pueden convertirse en *información* para mejorar la toma de decisiones tanto del sector público, como para mejorar el modelo de negocios de cualquier tipo de empresas, a través de recomendaciones personalizadas, marketing estratégico, proyecciones de inventario *inteligentes*, etc. Téngase en cuenta que en todas las empresas basadas en datos, el costo marginal es \$0. Incorporar miles de clientes nuevos no demanda inversión adicional al mismo nivel y del mismo modo que en una empresa industrial tradicional. Una vez que la tecnología está desarrollada (plataforma, algoritmo, etc), el costo marginal es casi \$0.

3.5.1.10.4.2. Descripción, predicción y prescripción

El *Machine Learning* tiene:

- i) una parte *descriptiva* (lo que ha pasado): esto analiza el pasado en función de datos recopilados;
- ii) una parte *predictiva* (lo que va a pasar): acá se usa la *Machine Learning* para, en base al tratamiento de los datos del pasado, contruir modelos para *predecir* el futuro; y
- iii) una parte *prescriptiva* (lo que se quiere que pase): esta parte del ML no está aún madura, está en desarrollo, aquí la máquina no sólo predice el futuro sino que toma decisiones, o ayuda a tomar decisiones.

3.5.1.10.4.3. Breve historia de la Inteligencia Artificial. La Singularidad

Hechas las aclaraciones terminológicas de rigor, hagamos ahora un poco de

historia. El *Machine Learning* es un tipo de Inteligencia Artificial, y ésta tiene ya 70 años de edad y de desarrollo. La IA arrancó en 1956 con John McCarthy, el mejor discípulo de Alan Turing [\[1443\]](#) y Marvin Minsky [\[1444\]](#), pero hubo dos décadas en que no hubo ni inversión ni investigación, con lo cual son, en realidad, unos 50 años de desarrollo efectivo en materia de Inteligencia Artificial. La definición actual de AI es la que plantea que no se podrá diferenciar a un humano de la máquina. Esa imposibilidad de diferenciación, es lo que se llama *Strong AI*, también conocida como la *singularidad*. Verdaderamente, no se sabe a cuánto estamos de ese punto en el desarrollo de la AI. Donde sí se ha avanzado mucho a nivel IA es en tratar grandes cantidades de datos y *descubrir patrones numéricos y estadísticos* a través del ML y el BA. Hay una percepción generalizada (y errada, por cierto) de que estamos cerca de la singularidad, pero en realidad estamos muy lejos. Y tampoco estamos seguros de querer llegar a tal punto: Stephen Hawking afirmaba:

“The development of full artificial intelligence could spell the end of the human race” (...) “It would take off on its own and re-design itself at an ever increasing rate. Humans, who are limited by slow biological evolution, couldn’t compete, and would be superseded.” Hawking has been voicing this apocalyptic vision for a while. In a May column in response to *Transcendence*, the sci-fi movie about the singularity starring Johnny Depp, Hawking criticized researchers for not doing more to protect humans from the risks of AI. “If a superior alien civilisation sent us a message saying, ‘We’ll arrive in a few decades,’ would we just reply, ‘OK, call us when you get here—we’ll leave the lights on’? Probably not—but this is more or less what is happening with AI” [\[1445\]](#)

No hay que preocuparse mucho por la singularidad. Estamos demasiado, demasiado lejos. En efecto, la IA aún no puede aprender de manera *incremental* en redes neuronales. Google tiene una IA que puede detectar un gato en una imagen, pero para entrenarla a reconocer un perro, la IA debe

desaprender cómo reconocer un gato. Es decir, no puede combinar de manera incremental reconocer imágenes de gatos y perros. Por eso estamos lejos de una *Strong IA*, y también lejos de la singularidad.

Ray Kurzweil, el Director de Ingeniería de Google, cree que la singularidad se alcanzará en 2045^[1446]. Su pensamiento presupone que es posible aplicar la teoría exponencial a la IA, con lo cual la evolución de la AI no sería lineal sino exponencial, y ello es lo que, a su turno, permitiría llegar a la *singularidad*. La exponencialidad, se afirma, podría alcanzarse gracias a la mayor capacidad de cómputo, ya que cada 18 meses el número de transistores que entran en un chip se dobla. Ya se está llegando a los límites atómicos del silicio, por lo que ya se está explorando el grafito^[1447]. Y, además, por la computación cuántica, que computa en *Qbits*, una nueva forma de computar, en lugar de 0 y 1 en bits, y que permite tratar mucha más cantidad de información.

Ahora bien, no debe confundirse Ciencia y Tecnología. La tecnología sí es exponencial, pero la ciencia *sigue siendo lineal*. Los algoritmos aún no pueden aprender incrementalmente. Sólo aprenden de manera focalizada, y este aprendizaje, se llama *Weak, Narrow, o Applied AI*. Algo muy distinto de una *Strong AI*. Además, la forma de aprender de la IA y del ML, es mediante algoritmos inventados hace 40 años, en la década del '80. Las ideas básicas son, en sí, viejas.

3.5.1.10.4.4. *Inteligencia Artificial vs. Machine Learning*

¿Pero qué es lo distinto entre IA y ML? Cuando un algoritmo aprende reglas de asociación que le son enseñadas por algún experto humano, tal enfoque de aprendizaje automático se dice que es *top-down*. Todos los métodos de aprendizaje que usa la AI son *top-down*. En cambio, en el ML, es el propio algoritmo el que deduce las reglas, extrae patrones, en función de los datos, con un enfoque *bottom-up*. Ningún experto le enseña al algoritmo las reglas, éste las descubre de modos que el humano puede no entender. De allí que se diga, coloquialmente, que la *Máquina Aprende*, sin que nadie le enseñe.

Desde este punto de vista, el ML es una herramienta más de la AI, que utiliza algunos algoritmos que son de tipo *top-down*, i.e. requieren de un experto que le enseñe al ingeniero que, a su turno, codifica el algoritmo –esto se denomina *Supervised Learning* [\[1448\]](#) –; mientras que en ML *no se requiere el experto*, ya que el mismo algoritmo extrae las reglas, las funciones, los patrones –esto se denomina *Unsupervised Learning* [\[1449\]](#) – y, como se dijo, el enfoque es distinto al ser *bottom-up* [\[1450\]](#) .

Ambos procesos de aprendizaje se basan en una serie de algoritmos genéricos pre-establecidos, que tratan los datos con los que se entrenan, y de los datos, extraen *conocimiento*: (i) *logistic regression*; (ii) *linear regression*; (iii) *decision tree*: algoritmo considerado *explainable-AI* (XAI) [\[1451\]](#) , i.e. explica cómo llega a la predicción que llega, algo más se dirá sobre esto más abajo–; (iv) *Bayesian networks*; (v) *K-means (Clustering)*; (vi) *neural network*: algoritmo considerado *non-explainable AI* –más abajo se vuelve sobre el punto–; y (vi) *deep learning*: también es un modelo de *non-explainable AI*, las predicciones son muy buenas pero no explica cómo se llega a la predicción.

Estos siete algoritmos *son por ahora todo lo que hay* en materia de AI. No tiene sentido desarrollar nuevos algoritmos, salvo que seas una empresa de tecnología de punta [\[1452\]](#) . Hay que usar alguno de estos siete *artefactos*, y combinarlos.

3.5.1.10.4.5. *El Data Scientist*

Es el *Data Scientist* el profesional que sabe y asesora cómo ingresar los distintos datos que se dispongan, en alguno de estos siete algoritmos, para obtener el mejor conocimiento volcado en reglas. Recuérdese, entonces, que en el ML, la máquina elabora su propia regla luego de analizar los datos tratados. Pero los datos deben contener la regla en ellos, para que la regla que se extraiga sea útil.

3.5.1.10.4.6. *El impacto laboral de la IA*

En otra orden de ideas, y mirando un poco hacia el futuro no tan cercano, 2030, 2035, cualquier tarea que pueda ser automatizada o medida por eficiencia, será en ese entonces realizada ya por máquinas. Todo lo que no pueda medirse por eficiencia, no será realizado por máquinas. Las habilidades manuales quedarán protegidas, e.g. un jardinero. También los trabajos creativos y artísticos. Pero todos los demás serán, sin dudas, reemplazados. A mediano plazo, siempre una nueva tecnología primero destruyó trabajos, pero luego se crean nuevos trabajos que son, en cantidad, muchos más que los anteriores. La IA afectará a todas las industrias, y eso es nuevo; además, el cambio es muy rápido, lo que no da mucho tiempo para prepararse e incorporar nuevas habilidades.

3.5.1.10.4.7. *Explainability*

En materia de ML, *transparencia* es sinónimo de *explicación*. *Explainability* [\[1453\]](#) quiere decir que es importante entender cómo el algoritmo llega a un resultado determinado. Por ejemplo, en materia bancaria, esa transparencia implica divulgar las razones por las cuales se ha producido la denegación *online* de un préstamo, lo que implica que no podrían usarse en materia bancaria aquéllos algoritmos que sean del tipo *non-explainable*. Muy vinculado a la explicabilidad, están los sesgos: muchos datos se han recopilado *en origen* con sesgos, porque fueron cargados por personas *sesgadas*, con lo cual el sesgo se trasladará al ML, y por ende el resultado también será *sesgado*. Ya ha habido ejemplos de algoritmos usados por la banca, que terminaron teniendo comportamientos racistas al ser entrenados con datos sesgados [\[1454\]](#). Se vuelve sobre esto *infra*.

Evidentemente, el campo del *Unsupervised Learning* presenta (importantes) desafíos, toda vez que no se requiere *un experto* del dominio (vs. enfoque *top-down*) para crear un modelo, o entender el resultado. Además, el mismo algoritmo puede servir para distintos dominios: predice datos futuros en función de datos pasados. Esto es programable, y escala muy bien a medida que crece la cantidad de datos disponibles. Ahora bien, en el aprendizaje automático supervisado el algoritmo va descubriendo en base a

los ejemplos de datos con los que se lo entrena. Aparece aquí la noción de *predictores*, cuya configuración es una materia práctica muy complicada, propia también del *Data Scientist*: si los datos no son suficientes, o si están muy *sucios*, el predictor no funcionará bien. Pero lo bueno es que todos los modelos supervisados se pueden evaluar, se puede medir su *performance* en cada dominio de aplicación, pero no debe olvidarse que por definición *todos los algoritmos por naturaleza son erróneos, porque están prediciendo cosas que no han pasado aún*. Por eso es tan importante evaluarlos, para saber si ese *grado de error* es aceptable en el dominio del que se trate. No es lo mismo el error de predicción en materia climática, que financiera, que de salud de las personas, o de flujos marítimos y ocupación futura de puertos. El ajuste del algoritmo se produce agregando o limpiando o cambiando predictores, es decir, datos. El modelo de aprendizaje se puede entrenar diariamente, semanalmente, mensualmente, según como evoluciona el sector en el que se aplica. El entrenamiento toma forma de “*feature engineering*” ^[1455]. Al entrenar un algoritmo, generalmente se afina la calidad del *predictor*, antes que agregar datos. Siempre hay un punto en el ML donde más *cantidad* de datos, no añade más *calidad* de datos.

Veamos ejemplos de todo lo anterior. En AI, en un algoritmo de aprendizaje tipo *top-down*, trabajan juntos un médico con un ingeniero que codifica. En cambio, en ML, con enfoque *bottom-up*, el algoritmo *se basa en y aprende de* los datos, pero no se recurre al médico ni al experto *del dominio* para enseñar o entrenar al algoritmo. El algoritmo aprende de los datos, los modelos son genéricos, y es, también, *una nueva forma de programar*, donde se reduce el costo de programación. En efecto, en la computación tradicional el ingeniero debe programar todo, de manera explícita, anticipada y determinista. Esta forma de programar es la seguida, por ejemplo, para escribir un *Smart Contract*, y está presente en cualquier app descargada en Smart Phone: repárese en que existen aproximadamente 12 millones de líneas de código de programación en cualquier teléfono inteligente en la actualidad. Todo es determinista y previamente programado. En cambio, en el ML propiamente dicho, no supervisado por un experto, no se programan todos los casos previamente, sino que la computadora, a través del algoritmo, puede aprender de los datos, sin ser programado previamente. Es decir, nuevos

datos, te dan nuevos conocimientos, sin necesidad de re-programar. Es innegable que es *per se* una nueva forma de programar, es una nueva filosofía y esto es realmente revolucionario.

3.5.1.10.4.8. El Gobierno del Dato y el Feature Engineering

Ahora bien, si los datos son el nuevo petróleo, entonces los *Data Scientists* son los nuevos Jonh D. Rockefeller. Ello es así ya que la *preparación* de los datos para encarar un proyecto de ML es esencial e insume el 80% del tiempo y del esfuerzo en un proyecto de ML. Es aburrido, es tedioso y es mucho, mucho trabajo, además de ser muy costoso, y puede llevar años.

En primer lugar, encontrar el dato adecuado puede ser muy complicado en algunas empresas. Por ejemplo, los bancos pueden tener diez silos de datos distintos, adquiridos incluso por compra de otros bancos más pequeños. Estos datos, donde sea que estén, son el *input* en ML y este *input* es siempre en formato tabular (filas: unidad de análisis; columnas: objetivo de predicción). Una *data warehouse* tiene distintas bases de datos dentro, con distintos *lenguajes* cada base. Por ejemplo, Deutsche Bank tiene 46 data warehouses. As vez, hay datos internos de la organización y también datos externos (públicos: gratis y privados: pagos) que pueden ser útiles para completar el modelo, e.g. datos generados en smart cities, en previsiones climáticas, en google news, en yahoo finance, wikipedia, IMDB, en kaggle, un repositorio público de datos para ML bien tratado [\[1456\]](#), etc. Hay muchos repositorios externos.

En segundo lugar, hay que combinar los datos. Combinar los datos en una sola tabla: todos los datos deben tabularse. Esta construcción de tablas en el *ML* es complicada. Las filas son las unidades de análisis y las columnas son los *predictores*. A veces una hoja de Excel sirve, pero no es fácil combinar todas las bases de datos. Luego hay que explorar el dato: calcular medianas, medias, a modo de primer conocimiento exploratorio. Una vez construida la tabla, lo que se hace es un *sanity check* [\[1457\]](#): corroborar si lo que hay en la tabla es lo que quería tener en la tabla.

En tercer lugar, la limpieza de datos es muy importante. Hay que borrar

filas y columnas duplicadas, y en los descriptores/atributos/campos hay que borrar los atributos que no tienen suficiente información para una unidad de análisis, identificadores (DNIs, dirección, etc, tampoco suelen servir), al igual que los nombres de las personas. El ejemplo clásico es corregir acentos que faltan, y letras mayúsculas o minúsculas que tienen que coincidir. Cuando el dato proviene de distintas bases de datos, estos problemas son muy frecuentes y el algoritmo tomará como valores distintos palabras con o sin acentos. También deben borrarse los atributos o descriptores que no tienen valor para la predicción, porque pueden añadir *ruido* a la predicción. Hay atributos que no sirven al fin determinado (por ejemplo, códigos de reservas, etc.) Hay atributos que están correlacionados entre sí: cliente bancario con activos/ingresos por X valor, y la deuda que tiene con el banco. Lo que interesa puede ser la relación ingresos-deuda, que son dos *features* importantes. Pero hay *features* que no importan para el modelo, entonces pueden ser eliminados. El paso del *Raw Data* al *Clean Data* genera menos unidades de análisis y menos campos por cada unidad. Es el *Data Scientist* quien también debe decidir qué hacer con los valores que faltan, o con los valores extremos.

En cuarto lugar, una vez *limpiado* o *completado* el *data set*, empieza el baile, el *Feature Engineering* (FE), o Ingeniería de Atributos, el proceso de creación de descriptores del modelo: son las columnas de la tabla, y la decisión sobre qué columnas crear para que el modelo funcione mejor, de acuerdo a los datos que son el *input* para predecir un *output*. En este momento, es donde hace falta entender muy bien el negocio o ámbito en el que se está aplicando el modelo de ML, y hay que ser creativo para crear los predictores. El FE es un proceso iterativo, recursivo. Se crea el atributo, se lo modela, se aprecia cuál es el resultado de la predicción, y si la calidad es buena, se para ahí; si no es tan buena, se vuelve a ajustar el modelo, a través de los predictores, y así sucesivamente. Pero se debe saber cuándo parar, ya que siempre el ML será siempre *erróneo*, recordar que está prediciendo futuros.

Todo este proceso de creación de *features* no se puede automatizar todavía, se hace de manera manual. Es necesario que el técnico esté sentado junto con el *Business Owner*, pensando la creación de *features* para que el modelo a ser creado funcione del mejor modo posible. Hay *features* que son muy específicos del sector en que se usa el ML: por ejemplo, ventas / tamaño de la

tienda; ingreso familiar/tamaño familiar; transformar un número en un dato categórico (agrupar en valores bajos, medios y altos).

En quinto lugar, el *Data Scientist* debe también determinar qué modelo usar, en función de los datos disponibles, y del *outcome* deseado. Los modelos existentes son los algoritmos arriba descritos. Los algoritmos que existen son los que hay, y el conocimiento que extraen de los datos, es lo que se denomina “*modelo*”. Hay modelos supervisados y no supervisados que se aplican automáticamente. En el caso de árbol de decisión, por ejemplo, las reglas se van *explicitando* y permiten conocer mejor el ámbito o negocio, de un modo que antes era sólo intuitivo y netamente humano. Ahora bien, cada modelo, cada algoritmo, produce resultados distintos, y estos resultados pueden compararse, interpretarse. En función del conocimiento extraído, se ajustan los objetivos, se limpian o cambian datos o predictores, o simplemente no se lo usa más porque no sirve al negocio o ámbito. Interpretar el modelo nos permite compararlo con otros, y estimar la performance. Normalmente, se crea un modelo con el 80% aleatorio *de todos los datos disponibles*, y el 20% restante se lo separa, y no se lo usa para crear el modelo, sino para testear sus resultados: como ya se tienen los datos del pasado (descriptores), puede validarse contra ese 20% si la predicción sobre el pasado es cierta porque coincide, o si no es cierta porque no coincide. Si la predicción hacia el pasado se valida y coincide con lo que ha ocurrido, entonces el algoritmo puede generalizar datos para el futuro.

3.5.1.10.4.9. Problemas de regresión y problemas de clasificación

Remarcada la importancia del gobierno del dato, su limpieza y la FE, volvemos a los algoritmos propiamente dichos, XAI vs. *non-explainable AI*. En los modelos “no explicables”, el modelo es una caja negra, no explica cómo llega al conocimiento extraído (e.g. algoritmos de tipo red neuronal). Por ende, en algunos sectores, tal modelo que no es explicable no puede ser utilizado, por ejemplo, para el *scoring* bancario. No puedo no informar la razón por la cual no se otorga un crédito al cliente.

A su vez, se marcó antes que existe ML supervisado y no supervisado. En el ML supervisado (e.g. el árbol de decisión) cuando intentamos predecir un número (importe de ventas, cantidad de unidades, propensión de algo),

estamos solucionando *un problema de regresión*. Existe cuatro o cinco algoritmos de regresión [\[1458\]](#), conocidos desde la década del 1980. Esto es ciencia y no hay nada nuevo en esto. Lo que sí hay es más poder de cómputo, lo que permite que las redes neuronales sean más potentes, procesen más datos, con cada vez más datos digitalizados, etc. Ahora bien, si queremos predecir una *categoría*, y no un número (si el paciente tiene diabetes, si la empresa va a quebrar, o si el préstamo se va a pagar), lo que estamos haciendo es solucionar *un problema de clasificación* [\[1459\]](#). Existen cuatro o cinco algoritmos que resuelven estos problemas de clasificación. Según si el problema a resolver es de regresión o de clasificación, existen distintos modelos a aplicar.

En efecto, si queremos resolver un problema *de regresión*, que nos arroja un número, podemos calcular el error con el 20% de datos separados para tests, a nivel de error medio para todo el conjunto de los datos. El modelo de regresión que me de un error medio menor, será un mejor modelo que los demás. El problema es que puede haber mucha dispersión entre el máximo y el mínimo de los errores; entonces nos interesa exagerar los máximos y los mínimos. Por eso se elevan al cuadrado, para exagerar los errores grandes y reducir los errores pequeños: *Mean Square Error* (MSE) [\[1460\]](#).

Ahora bien, si queremos resolver un problema de categoría, y no numérico, ¿cómo se calcula el error del modelo vs. otros modelos? En los modelos de categoría, para evaluar su performance, se utilizan cuatro posibilidades: true negative y true positive; false negative y false positive.

Hasta aquí en esta *disgresión*, se ha analizado muy someramente cómo funciona, en la realidad, el ML como tecnología *experimental*, con un enfoque de aprendizaje automático basado en datos de tipo *bottom-up*, distinto al enfoque *top-down* de la AI. Ahora bien, dentro del ML, existe un modelo conocido como *Deep Learning*, i.e., un algoritmo particular, del tipo de red neuronal, que se utiliza mucho para el reconocimiento de imágenes. Es un tipo de ML *supervisado* pero *non-explainable*. Sirve para problemas muy específicos, funciona muy bien estadísticamente, pero no hay forma de interpretar el resultado que se obtiene. El *Deep Learning* permite tratar datos

sintéticos: el conjunto de datos que no pertenece a ningún cliente, pero permite extraer y conocer los patrones de conducta de los clientes. Así, se contruyen algoritmos que crean *data sets* sintéticos, con un enfoque multidimensional que crean *miles de relaciones entre los datos reales*. Estos datos sintéticos se crean a través de IA, con algoritmos, y son a la vez realistas (tienen los patrones reales), y representativos (pero con una identidad ficticia). El *data set* se arma aleatoriamente, y se crea un modelo con datos sintéticos. Esto sería una revolución completa en el campo del ML ya que los datos sintéticos solucionan el problema de la privacidad, pero no solucionan el problema de los *sesgos*.

3.5.1.10.4.10. *Unsupervised Machine Learning*

En otro orden de ideas, y entendiendo que el ML *supervisado* (SML) resuelve solo dos tipos de problemas: regresión (predice un número) o clasificación (existen instancias categóricas, no numéricas), debe entenderse también que en el ML no supervisado (*Unsupervised Machine Learning*, o UML) [\[1461\]](#), no se sabe qué se está buscando, no se quiere predecir una columna específica, sino que *se busca extraer reglas o asociaciones*. Así, el análisis es multi-dimensional (miles de filas y columnas). El UML es más difícil de entender que el SML, que busca predecir un atributo en concreto. En UML no se predice algo, y eso implica que no se puede evaluar su *performance*, a diferencia del SML, que permite comparar con los resultados obtenidos por otros modelos de SML. En UML, sólo se pueden *interpretar* las reglas que se extraen, pero no se puede evaluar su *performance*. El ejemplo típico del UML es el marketing estratégico. El UML se utiliza mucho para detectar anomalías, es muy importante para detectar el fraude bancario. También se usa UML para segmentar clientes. Y se pueden vincular: se puede crear el UML para construir *etiquetas* de grandes cantidades de datos, que luego, a su vez, son usadas como *input* del SML para un modelo predictivo específico. El UML también se utiliza para recomendaciones. Los algoritmos de UML son actualmente cuatro: *clustering*, *anomaly detection*, *association rules*, *topic modeling*.

Finalmente, debe informarse al lector que ha llegado hasta aquí que los

(nuevos) problemas generados por los sesgos en datos y de los algoritmos con ellos entrenados han dado lugar a una nueva disciplina, que se denomina *Ética de la IA* ^[1462]. El punto de partida es un problema del ML y de la IA: los datos para entrenar los algoritmos vienen de un mundo *analógico*, ergo los datos ya vienen sesgados por las decisiones que han tomado los humanos que cargaron el dato en la base de datos ^[1463]. Como el algoritmo aprende de los datos viejos, puede incorporar el sesgo del dato *en origen*. Los algoritmos también pueden tener sesgos en su creación, ya que los crean personas o empresas con un sesgo determinado. Hoy por hoy, el diseño de un algoritmo y de los datos utilizados para entrenarlos cae normalmente dentro de la categoría de secreto industrial o comercial, con lo cual no se pueden auditar los modelos que se utilizan. Este (gran) déficit informativo busca ser compensado por legislación específica que obligue a cumplir ciertos criterios de transparencia cuando se utilizan algoritmos ^[1464].

3.5.2. *Criptoactivos, Contratos Inteligentes & Lege Ferenda: Análisis y crítica de legislación proyectada en Argentina*

Los reguladores argentinos –UIF, AFIP, BCRA y CNV– vienen analizando el fenómeno de los criptoactivos desde hace tiempo, en procura de una regulación inteligente ^[1465].

Sin embargo, lo cierto es que a Mayo de 2020 no existe un proyecto de ley formalmente presentado al Congreso de la Nación. Sí he tenido a la vista una serie de proyectos de ley que pretenden regular los criptoactivos, impulsados por nueve Universidades ^[1466] con el apoyo del Círculo de Legisladores de la Nación, en el marco de una simulación de *cambio de roles* donde los estudiantes universitarios oficiaron como Diputados virtuales. Desde ya, se trata de una muy loable iniciativa, mas hasta donde el autor pudo corroborar, ningún proyecto de los citados alcanzó estado parlamentario, lamentablemente.

IV. Cuestiones Contractuales, Judiciales y Responsabilidad Civil Emergente

4.1. Introducción

El ecosistema *blockchain* puede ser generador, en algunos casos, de una gran red contractual, que puede ser *a priori* legalmente calificada como una *conexidad contractual*, como se verá en el apartado siguiente. En efecto, el OBSERVATORIO Y FORO DE *BLOCKCHAIN* DE LA UNIÓN EUROPEA [\[1467\]](#) mapea las siguientes áreas de fuerte actividad contractual:

- 1) Plataformas de *blockchain*, incluyendo las redes de nodos que validan y agregan nueva información al registro distribuido, y distinguiéndose entre *blockchains* públicas y privadas;
- 2) Desarrolladores del software en formato *open source* (o no) de cada plataforma de *blockchain*, normalmente agrupados en entidades como la Fundación Ethereum, o la *Blockchain* Federal Argentina, o Alastria en España, incluyendo plataformas de desarrollo de *Smart Contracts*, como el caso de OpenLaw, o Aragon, o de desarrollo de Dapps y DAOs, como el caso *TheDAO* y su versión mejorada, *TheLAO*, y las relaciones contractuales que se celebran en su seno entre desarrolladores y usuarios;
- 3) Los *Exchanges* y *Wallets*, en tanto intermediarios entre *blockchains* y sus usuarios finales;
- 4) Las empresas de tecnología que ofrecen servicios de auditoría y due diligence sobre programas de software como los *Smart Contracts*;
- 5) Los usuarios finales de las *blockchains*, cualquiera sean sus clases, e incluyendo usuarios corporativos y gubernamentales en *blockchains* privadas o usuarios no corporativos en

blockchains públicas; y

6) Los gobiernos y autoridades regulatorias, en tanto terceros interesados y en muchos casos, actuando como nodos de algunas *blockchains*;

En algunas de estas áreas, los conflictos han llegado a ser judicializados –en temas vinculados a la responsabilidad civil de *Exchange* y *Wallets* ante un ciberataque y en *Smart Contracts* de *trading* algorítmico– y en otras es probable su judicialización próxima, como se verá en este Capítulo.

Ahora bien, antes de pasar a analizar en particular los distintos contratos que se utilizan en cada una de las seis áreas identificadas, nos detendremos en la red que los contiene, en la conexidad que los puede vincular, y que puede producir e implicar, *per se*, importantes consecuencias jurídicas bajo nuestro CCCN.

4.2. *La conexidad contractual*

La teoría de los contratos conexos es quizás la mayor innovación en materia contractual introducida por el CCCN ^[1468]. Con anterioridad a la sanción del CCCN, la doctrina y jurisprudencia argentina ya se refería a ellos con distintos términos: contratos coligados, redes contractuales, o grupos de contratos.

El art. 1073 CCCN los define así:

“Definición. Hay conexidad cuando dos o más contratos autónomos se hallan vinculados entre sí por una finalidad económica común previamente establecida, de modo que uno de ellos ha sido determinante del otro para el logro del resultado perseguido. Esta finalidad puede ser establecida por la ley, expresamente pactada, o derivada de la interpretación, conforme con lo que se dispone en el art. 1074.”

Andrés Sánchez Herrero conceptualiza sus dos notas características: (i) la autonomía de cada contrato: al menos se requieren dos contratos válidos para que exista conexidad –pueden existir más–, cada uno con su propia finalidad, que se embebe en una finalidad *común* que les da sentido a los contratos coligados; y (ii) tener una finalidad económica común, o *supracontractual*, previamente establecida, de modo tal que cada uno de ellos ha sido determinante del otro para el logro del resultado perseguido [\[1469\]](#). Agrega el autor citado que, si bien desde lo formal y sustancial existe una pluralidad contractual, la operación es económicamente unitaria, y esto afecta al principio relativo de los contratos. Así, en los contratos no conexos, o tradicionales, sus efectos no se proyectan más allá de las partes que lo celebran, mientras que en los contratos conexos, los efectos de los contratos pueden extenderse o proyectarse sobre el grupo de contratos, independientemente de que las mismas partes hayan celebrado todos los contratos.

Sánchez Herrero ilustra redes conexas de contratos *off-chain*:

- i) redes de comercialización como el caso de la agencia, la concesión, la franquicia;
- ii) los contratos principales y sus accesorios de garantía;
- iii) los contratos principales y los subcontratos;
- iv) la comercialización de bienes a crédito;
- v) los contratos previos y los contratos definitivos;
- vi) los contratos que integran el sistema de tarjeta de crédito;
- vii) los contratos de leasing financiero;
- viii) los círculos de ahorro;
- ix) los contratos de comercialización, mantenimiento y suministro;
- x) los contratos de venta de hardware, licencia de software y servicios de asistencia técnica;

- xi) los contratos de tiempo compartido;
- xii) los mutuos bancarios que incluyen garantía hipotecaria y seguro de vida por saldo deudor;
- xiii) los contratos del sistema de *Shopping Center*; y
- xiv) los contratos de un sistema de transporte multimodal [\[1470\]](#).

Yo sostengo que la celebración de un contrato inteligente *on-chain* puede normalmente ser un caso de conexidad contractual expresa o implícita –hasta tanto la legislación se refiera a ellos–, ya que pueden concurrir los siguientes contratos coligados entre sí:

- i) el contrato convencional subyacente que puede prever los términos y condiciones a ser programados en un *Smart Contract* de ejecución o de garantía;
- ii) el contrato de desarrollo de software para implementar una *blockchain* privada, incluyendo la licencia para su uso;
- iii) el contrato de licencia de uso de una *blockchain open source* pública o una privada;
- iv) el contrato de compra o venta de criptomonedas a un *Exchange*, y de custodia de llaves con una *Wallet*;
- v) el contrato de compra de tokens, tengan éstos fines funcionales –utility token– o de inversión –security token–, incluso de inversión derivada si el token deriva su valor de un activo subyacente o de inversión automatizada, si se tratase de DAICOs o *smart derivative contracts*; y
- vi) el contrato de licencia de uso de *Smart Contracts*, o de desarrollo y programación de un *Smart Contract* a medida, incluyendo los servicios de auditoría técnica sobre el código de programación, en su caso.

4.2.1. Clases y modalidades de contratos conexos

Se afirma que la finalidad común a los contratos conexos puede venir impuesta por la ley, o por un contrato expreso o implícito ^[1471]. Ejemplos de conexidad contractual impuesta por la ley son los art. 40 de la Ley N° 24.240 ^[1472] de defensa del consumidor y del usuario, o el art. 1 de Ley N° 25.065 ^[1473], que regula el sistema de tarjeta de crédito. Serían éstos dos ejemplos citados casos de conexidad típica, por cuanto la ley específicamente la ha regulado ^[1474].

En los demás casos, la conexidad puede surgir de un acuerdo entre las partes, expreso o tácito, debiéndose en éste último supuesto interpretarse en cada caso concreto los contratos involucrados, según el criterio del art. 1073, CCCN.

En punto a las modalidades, señala Sánchez Herrero que la conexidad puede ser genética, o funcional. En el primer caso, un contrato ejerce influencia en la formación del otro, como sucede entre los contratos *previos* y los contratos *definitivos*. La conexidad funcional, en cambio, puede ser unilateral o bilateral. Cuando es unilateral, un contrato es accesorio o auxiliar de otro, que es el *principal*, como por ejemplo la fianza respecto del mutuo, y por ende, las vicisitudes que afecten al principal repercutirán necesariamente en el accesorio. Por otro lado, cuando la conexidad es bilateral, los contratos son interdependientes pero no hay una relación de principal a accesorio entre ellos, por lo cual las vicisitudes que afectan a cualquiera de los contratos, pueden irradiar efectos a los demás contratos conexos bilaterales. Como ejemplo: contratos de provisión de hardware, licencia de software, y de prestación de servicios de asistencia técnica ^[1475]. A su vez, los contratos conexos pueden ser celebrados por adhesión a cláusulas generales, pueden ser contratos de consumo, o también ser contratos paritarios.

4.2.2. Efectos e interpretación de los contratos conexos

Los efectos típicos de los contratos conexos y la forma de interpretarlos vienen dados por el CCCN en sus arts. 1074 y 1075:

“Interpretación. Los contratos conexos deben ser interpretados los unos por medio de los otros, atribuyéndoles el sentido apropiado que surge del grupo de contratos, su función económica y el resultado perseguido.

“Efectos. Según las circunstancias, probada la conexidad, **un contratante puede oponer las excepciones de incumplimiento total, parcial o defectuoso, aún frente a la inejecución de obligaciones ajenas a su contrato.** Atendiendo al principio de la conservación, la misma regla se aplica cuando la extinción de uno de los contratos produce la **frustración de la finalidad económica común.**” (el resaltado es mío).

4.2.2.1. Excepción de incumplimiento contractual. Suspensión de cumplimiento

Como gran excepción al principio del efecto relativo de los contratos, la conexidad contractual postula que hay terceros que no son “*tan terceros*” –en palabras de Sánchez Herrero ^[1476] –, precisamente porque son parte de un contrato conexo que integra un grupo de contratos, y en tal carácter, pueden adquirir derechos o contraer obligaciones *de otro contrato del que no son, formalmente, parte*, pero que tiene una conexión con un contrato del que sí son, formalmente, parte.

Así, puede suceder que el contrato del que son parte se extinga por extinción del contrato conexo del cual *no son parte*; o que se deba responder civilmente respecto de una obligación contractual por la que no se es deudor contractual, pero sí *deudor conexo*; o que se les oponga la excepción de incumplimiento por un incumplimiento en el que no han participado, o que se habiliten acciones directas entre partes no contratantes, pero que integran una red contractual dada, en función de las circunstancias de cada caso.

Así, la suspensión del cumplimiento contractual por el incumplimiento de

otro contrato conexo –del cual el excepcionante puede no ser parte– está expresamente admitida, reconociéndose la interdependencia de las prestaciones en hipótesis de redes contractuales. Esto procederá, *según las circunstancias*, en dos casos: (i) ante el incumplimiento de una obligación nacida del mismo contrato cuyo cumplimiento se pretende suspender; y (ii) ante el incumplimiento de una obligación nacida de un contrato conexo [\[1477\]](#).

4.2.2.2. Frustración de la finalidad económica común

El art. 1075 refiere a la “finalidad económica común” en los contratos conexos, y permite que, frustrada que sea, tal frustración tenga efectos *expansivos* a los contratos coligados involucrados [\[1478\]](#). Señala Sánchez Herrero que si un contrato conexo se extingue *por cualquier motivo* [\[1479\]](#), y ello, a su turno, puede producir la frustración de la “finalidad económica común conexas” [\[1480\]](#), entonces, pueden considerarse extinguidos [\[1481\]](#) todos los contratos coligados, por haberse perdido la finalidad común que los justificaba. También analiza el autor citado el caso inverso: frustración de la finalidad económica común, sin extinción previa de alguno de los contratos coligados, y concluye que en tal caso la ley no autorizará la extinción expansiva, aunque *de lege ferenda* debiera modificarse la norma [\[1482\]](#) para admitir expresamente tal supuesto.

4.2.2.3. Resolución por incumplimientos conexos

Sánchez Herrero, con una envidiable claridad conceptual, aborda la álgida cuestión de si es posible *resolver* uno de los contratos conexos invocando el incumplimiento de otro contrato conexo [\[1483\]](#). O puesto en otros términos: ¿el incumplimiento de un contrato conexo tiene efectos expansivos a los otros contratos conexos? Puntualiza el autor citado que ello ocurre, por ejemplo, en

el art. 44 de la Ley N° 25.065 ^[1484]. Pero a falta de una ley que lo admita, qué opina, lector: ¿procede tal efecto expansivo del incumplimiento contractual conexo sin ley que lo disponga?

4.2.2.4. Deberes de cooperación y de conducta. Deberes respecto de “terceros”

Se afirma que en hipótesis de redes contractuales, los contratantes están, por virtud de la buena fe, obligados a cooperar para conseguir la finalidad económica común y sostener así el sistema, para que todas las partes se beneficien ^[1485], inclusive el organizador (e.g., el franquiciante, el concedente, el emisor de la tarjeta de crédito, el banco que concede financiamiento, etc.). Asimismo, se afirma que quienes deciden participar de una red de contratos organizada por otro, descuentan un deber de conducta de trato igualitario –en sentido de igualdad aristotélica– y de no discriminación hacia los integrantes de la red.

Asimismo, se afirma que las redes contractuales generan para sus partícipes obligaciones respecto de terceros –en el sentido de que, en algunos casos, no son parte cocontratante en todos los contratos conexos pero sí son “parte” de la red de contratos ^[1486].

4.2.2.5. Extensión de la responsabilidad

Salvo casos de expresa extensión legal de responsabilidad civil a otras partes integrantes de la red contractual, e.g., sistema de tarjeta de crédito o estatuto del consumidor, Sánchez Herrero afirma que los principios que guían la tipificación legal de la conexidad contractual genérica permiten, igualmente, extender la responsabilidad civil a otros miembros de la red de contratos, aunque ello no permite fijar una regla general de extensión de responsabilidad en todos los casos, sino que habrá que analizar los hechos de cada caso en concreto.

4.2.2.6. Interpretación de contratos conexos

Finalmente, a los contratos conexos se les aplican las reglas generales de interpretación del contrato, y, además, la regla específica del art. 1074, CCCN: interpretar los contratos conexos los unos por medio de los otros, atribuyéndoles el sentido apropiado que surge del grupo de contratos, de su función económica y del resultado perseguido, a lo que cabe agregar el criterio de interpretación de las situaciones jurídicas abusivas fijado en el art. 1120, CCCN, por aplicación analógica [\[1487\]](#).

4.3. contrato para programar un Smart Contract: Aspectos controvertidos

El contrato por el cual una parte, comitente, encarga a otra, contratista, la programación de un contrato inteligente es un contrato de obra intelectual, tipificado por el art. 1251, CCCN [\[1488\]](#), que puede ser oneroso o gratuito.

Se trata de un contrato bilateral –aunque será unilateral si es gratuito [\[1489\]](#)–, nominado, conmutativo –aunque puede, en algunos casos ser considerado aleatorio–, no formal, y habitualmente de ejecución sucesiva [\[1490\]](#), por el cual el comitente contrata al contratista para recibir un resultado eficaz, reproducible o susceptible de entrega, propio de una obligación de resultado, que se materializará en la producción y testeado de líneas de programación en un determinado lenguaje –una obra intelectual materializada en código de programación [\[1491\]](#)– para una determinada *blockchain*, tanto en código fuente –legible por humanos–, como en código objeto –legible sólo por máquinas–.

Lo anterior implica que la responsabilidad del contratista, en tanto sea una empresa dedicada a ofrecer servicios de programación [\[1492\]](#), será objetiva por ser de resultado su obligación [\[1493\]](#). En este contrato, el comitente pretende obtener un resultado material, con una utilidad concreta que se deriva del trabajo y de la actividad de *alto expertise* del contratista. La obra, el

software, se independiza del contratista y puede ser utilizada de manera reproducible por el comitente [\[1494\]](#) .

Así, puede postularse que la provisión informática es una actividad que, por lo común, supone la adquisición de un equipo de determinadas características, de un programa o software que cumple ciertas funciones, de un sistema en red o, en general, de bienes y servicios que solucionen determinados problemas de tratamiento de la información que maneja el requirente o usuario.

Desde tal perspectiva, el comitente o usuario espera un resultado funcional útil que derive de la aplicación de la máquina, el programa de su actividad, el sistema, red, bien o servicio informático de que se trate. En los términos indicados, la utilidad perseguida por el requirente o usuario es en sí mismo un objetivo que está presente no sólo en la provisión del hardware o del software, sino también en el contrato de mantenimiento y otros propios de la actividad de quien provee bienes o servicios de informática. El proveedor –i.e. el contratista-, ofrece una máquina, un sistema, bien o servicio informático basándose en la utilidad que brinda, y el adquirente busca satisfacer una necesidad funcional. Bajo tal entendimiento de cosas, la doctrina y la jurisprudencia coinciden en cuanto a que el proveedor informático contrae una “obligación de resultado”, que se traduce en asegurar la aptitud de tales elementos a los requerimientos hechos por el cliente para que con ellos este último llene la utilidad que persigue.

Cabe recordar, en este punto, que las “obligaciones de resultado” son aquéllas en las cuales el deudor está obligado a asegurar una finalidad determinada y ello implica cargar sobre el contratista la prueba de la causa ajena para eximir su responsabilidad. Dicho con otras palabras, por estar en juego “obligaciones de resultado” en las que el deudor asegura el logro del interés final pretendido por el acreedor, basta a este último demostrar la falta de obtención de ese interés, es decir, el mero incumplimiento material o estructural de la obligación asumida, para que, al igual que en cualquier hipótesis de responsabilidad objetiva, surja una presunción de adecuación causal contra el deudor [\[1495\]](#) .

4.3.1. Especificaciones y funcionalidades a cumplir por el Smart Contract. Arquitectura del software

La programación de un contrato inteligente se realiza de acuerdo a ciertas especificaciones esenciales, dadas por el comitente, y que explican y guían la arquitectura del software, las elecciones de diseño, y el proceso de construcción del mismo [\[1496\]](#). En esta etapa, el *expertise* para definir la (más) correcta arquitectura para un software dado que ese es el campo de actuación profesional de los llamados *Software Architects*. Se ha definido la arquitectura del software como:

“Software application architecture is the process of **defining a structured solution that meets all of the technical and operational requirements, while optimizing common quality attributes such as performance, security, and manageability.** It involves a series of decisions based on a wide range of factors and each of these decisions can have considerable impact on the quality, performance, maintainability, and overall success of the application [\[1497\]](#).” (el resaltado es mío)

El concepto es muy relevante, ya que así como un software debiera tener un diseño muy premeditado por su arquitecto, lo mismo puede predicarse respecto de las *blockchains*. Una mala arquitectura en el software produce, en potencia, lo mismo que una mala arquitectura en una obra, o quizás más técnicamente, lo mismo que construir un edificio sin el debido cálculo estructural y de fundaciones que suele (y debe) confeccionar un ingeniero civil. Todos los que ingresen al edificio así construido, corren riesgo. Lo mismo puede ocurrir en el software respecto de sus usuarios.

Así, lo que el arquitecto defina como estructura en función de su conocimiento y *expertise*, será luego construido literalmente por ingenieros y desarrolladores liderados normalmente por un *Project Manager*, que a veces puede ser también el arquitecto, aunque lo normal será tener un arquitecto,

que fija la estrategia del desarrollo, y un Project Manager que se ocupa de las decisiones tácticas dentro de la estrategia ya fijada [\[1498\]](#). Cae de maduro que el arquitecto es, a todas luces, un jugador esencial, ya que se supone que conoce y puede decidir sobre:

“...between platforms, languages, frameworks, libraries, paradigms, patterns, and tools, and (...) know what is available and where or how it fits into your ecosystem. They can help by analyzing and ruling things out, thereby eliminating options and narrowing the focus (...) the challenge becomes knowing what is available, how mature it is, what it’s good at, where it’s headed, and how well it suits the given problem domain from the longer-term perspective (...) Software architects play an important role in the early stages of the software development life cycle (SDLC), and they are ideally highly active in execution and delivery stages as well. They work in a **critical liaison role, helping the business and technical teams work together toward a common vision while addressing needs to meet stated goals within given constraints (budget, time, infrastructure, etc.)**. Architect is a role, not necessarily a rank, although it does require a high degree of technical experience and expertise, coupled with strong soft skills including influence, involvement, and leadership across a broad array of different areas (technical and functional).

The architect’s job is to guide, not dictate or mandate. An architect is not a “super-senior” developer. The title is often used as a promotional rank at the top of the developer hierarchy. This isn’t quite the right way to frame it; rather, it is a tangential **job function requiring a distinctly separate, broadened skill set in addition to senior developer skills**. Just like not all developers are on a career path to manager, not all developers are necessarily on the path to architect. Architecture is its own discipline and should be approached as a career change. Architects require a great deal of breadth of technical

knowledge to guide decision making. A large part of that breadth occurs in the form of understanding the various options, so they can pick the best tool, language, or method for the problem balanced against known constraints. An architect must exhibit management and leadership skills to successfully fulfill the duties of the role. **The Architect's responsibility is for the integrity of the entire system and satisfying business goals while mitigating risks.** They need to define and guide early, the things that are difficult/expensive to change later and **ensure that the business needs and pain points are properly addressed by solving the right problems.** Architecture **requires a holistic view** to see the big picture and understand how the software system works from a high level, **while also getting deep into the implementation details** (ability to zoom in and out, as needed).”^[1499] (el resaltado es mío)

Finalmente, existen arquitectos especializados en distintos campos del conocimiento, algunos de ellos, son: Enterprise Architecture, Systems Architecture, Software Architecture, Data Architecture, Business Architecture.

Volviendo a las especificaciones esenciales dadas por el comitente, y que explican y guían la arquitectura del software, dichas especificaciones se expresan por escrito en un documento coloquialmente denominado *Specs* (por *specifications*), más o menos extenso, que será un anexo muy importante del contrato de desarrollo, y que va vinculado a otro documento que estipula los plazos e hitos de desarrollo en el tiempo, normalmente adjunto como otro anexo del contrato. El éxito o el fracaso de cualquier programa de software a ser desarrollado de cero dependerá de la claridad, precisión y profesionalidad con la que las *Specs* sean escritas, o en su caso, acordadas, entre el comitente y el contratista. La versión definitiva del código programado, debiera cumplir íntegramente lo pactado en las *Specs*, y en este estado, no debieran quedar defectos visibles de programación, *bugs*.

Las variaciones de las especificaciones funcionales de un contrato inteligente, como cualquier variación del proyecto en un contrato de obra,

requieren por regla el consentimiento escrito del comitente, y no pueden ser modificadas de manera unilateral por el contratista, máxime cuando la forma de retribución es habitualmente *time & material*, i.e., coste y costas.

Ahora bien, excepcionalmente, si las modificaciones obedecen a eventos o circunstancias que no han podido ser previstos al celebrarse el contrato, y son necesarias para ejecutar la obra –i.e., programar el *Smart Contract*– conforme a las reglas del arte –o, por qué no, a nuevos requerimientos regulatorios–, entonces tales modificaciones podrán ser decididas por el contratista, comunicando la necesidad al comitente y estimando su costo, y el comitente podrá extinguir el contrato dentro de los diez días si tal variación implica un aumento del costo mayor al 20% [\[1500\]](#).

4.3.2. *El Decreto 165/1994 del Poder Ejecutivo de la Nación*

El 3 de Febrero de 1994 se publicó en el Boletín Oficial el Decreto 165/1994 que estableció un régimen especial para el registro de software por ante la Dirección Nacional de Derecho de Autor, al amparo de la Ley N° 11.723 de Propiedad Intelectual. En lo pertinente, el Decreto dispuso:

“Art. 1° -- A los efectos de la aplicación del presente decreto y de la demás normativa vigente en la materia:

a) Se entenderá por obras de software, incluidas entre las obras del art. 1° de la Ley N° 11.723, a las producciones constituidas por una o varias de las siguientes expresiones:

I. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación;

II. Los programas de computación, tanto en su versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por el computador;

III. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o

mantenimiento de software.

b) Se entenderá por obras de base de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.

c) Se considerarán procedimientos idóneos para reproducir obras de software o de base de datos a los escritos o diagramas directa o indirectamente perceptibles por los sentidos humanos, así como a los registros realizados mediante cualquier técnica, directa o indirectamente procesables por equipos de procesamiento de información.

d) Se considerará que una obra de software o de base de datos tiene el carácter de publicada cuando ha sido puesta a disposición del público en general, ya sea mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente o mediante la oferta generalizada de su transmisión a distancia con fines de explotación.

e) Se considerará que una obra de software o de base de datos tiene el carácter de inédita, cuando su autor, titular o derechohabiente la mantiene en reserva o negocia la cesión de sus derechos de propiedad intelectual contratando particularmente con los interesados.”

La definición de software provista por el referido decreto constituye el objeto de un contrato de obra intelectual, por el cual el comitente encarga al contratista la programación de un contrato inteligente que cumpla determinadas funcionalidades, las que debieran ser descritas muy minuciosamente en las especificaciones, o incluir adecuadas referencias a otros softwares que sirvan de ejemplo.

Así, el código del *Smart Contract* a programar i.e., a entregar, normalmente incluirá los diseños, tanto generales como detallados, del flujo lógico de los datos –esto es normalmente conocido como la arquitectura del software, equiparable *mutatis mutandis* a la idea de partido en la arquitectura– en un sistema de computación, y las líneas de código que implementan tales flujos

lógicos, tanto en su versión "fuente"^[1501], principalmente destinada al lector humano, como también en su versión "objeto", destinada a ser ejecutada y legible sólo por el computador, así como toda la documentación técnica que *explica* su funcionalidad, y en su caso el soporte o mantenimiento del mismo, así como el entrenamiento para su correcto uso, en su caso.

Cuatro años después, en 1998, se sancionó la Ley N° 25.036, publicada en el Boletín Oficial el 11 de Noviembre de dicho año, que realizó varias modificaciones a la Ley N° 11.723 de Propiedad Intelectual. Así, (i) se incluyó expresamente –ahora por ley del Congreso de la Nación, para guardar las formas– al software dentro de la definición de obra protegida conforme a la Ley N° 11.723, (ii) se aclaró que las personas jurídicas o físicas cuyos dependientes sean contratados laboralmente para programar serán los titulares de los derechos de propiedad intelectual respectivos, salvo pacto en contrario^[1502], y (iii) se admitió el contrato de licencia de software como una forma típica de comercialización del software^[1503] ya desarrollado o programado y funcional.

Debe tenerse muy en cuenta que en el contrato de licencia, el licenciatarario reconoce la propiedad intelectual del licenciante y paga por el uso –conforme a las restricciones contenidas en la licencia^[1504] – del software. Contratar un software propietario mediante licencia es algo muy distinto a contratar, de cero, el desarrollo de un software con determinadas funcionalidades, mediante un contrato de obra como el que se está analizando en este apartado.

Se ha sostenido por nuestros Tribunales que la licencia de software es una forma de reconocer el aprovechamiento económico del derecho de autor, que tiene soporte constitucional en el art. 17, en el art. 2 de la Ley N° 11.723, la Ley N° 25.036, y en la Ley N° 24.425 que ratificó el art. 10.1 del Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC o TRIPS, en inglés), que dispone que los programas de ordenador sean programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna^[1505]. Por ende, el uso de

software propietario sin la debida licencia es una infracción al derecho de propiedad intelectual, lo que, a tenor del art. 45.1 del ADPIC, habilita a las autoridades judiciales para ordenar al infractor que pague al titular del derecho un resarcimiento adecuado para compensar el daño que éste haya sufrido debido a una infracción de su derecho de propiedad intelectual, causada por un infractor que, sabiéndolo o teniendo motivos razonables para saberlo, haya desarrollado una actividad infractora [\[1506\]](#).

Así, la ganancia que no pudo percibirse por el incumplimiento del deudor ha de ser, entonces, objeto de reparación. En este sentido, se ha definido al lucro cesante como las ventajas económicas esperadas de acuerdo a probabilidades objetivas debida y estrictamente comprobadas, lucro cesante que no se presume sino que debe ser objeto de demostración. De esta forma se evita que sea más rentable, en el caso, infringir el derecho de autor y los derechos conexos que observarlos, pues si el utilizador consigue un precio más bajo en juicio que negociando con el titular del derecho se alientan las infracciones [\[1507\]](#). Por tanto, ante infracciones de software propietario, se ha sostenido que el parámetro aceptable para cuantificar el lucro cesante por una infracción al derecho de autor consistirá en estimar cuánto hubiese pagado por la licencia [\[1508\]](#), y que el uso ilegítimo del software puede tener diversas consecuencias, pero no constituye a la firma que lo crea o comercializa en una suerte de socia de quien se sirve de él, a los efectos de participar en sus ganancias [\[1509\]](#).

4.3.3. *Recepción de la obra*

El comitente debe recibir la obra, en este caso, el código del *Smart Contract* programado, en ambos formatos, fuente y objeto. Es una obligación legal del comitente, con correlato en el derecho a liberarse de su obligación de entrega, en tiempo y forma, del contratista [\[1510\]](#), quien podría consignarlo judicialmente ante la omisión culposa del comitente de recibirla.

Afirma Calderón que la recepción de la obra es un tema trascendente, ya

que: (i) extingue la responsabilidad del contratista por defectos ostensibles y por diferencias de calidad si el comitente no hace reservas y (ii) marca el punto de partida del plazo de garantía de la responsabilidad por inadecuación de la obra [\[1511\]](#). Ello es así ya que la recepción de la obra tiene un efecto extintivo, al presumir que el comitente ha aceptado voluntariamente la obra, lo que implica que el comitente haya tenido la posibilidad de examinar la obra a fin de evaluar su conformidad con las especificaciones de programación pactadas y las consecuentes funcionalidades esperadas del contrato inteligente, y, además, la inexistencia de defectos aparentes, que en términos de programación, son los llamados *bugs*, para lo cual el comitente tiene derecho a verificar el desarrollo de los trabajos de programación, tanto durante como al finalizar la obra. Es también usual pactar una recepción provisoria de la obra, que no producirá los efectos propios de la recepción y aceptación, e iniciará un plazo pactado para comprobar la funcionalidad del contrato inteligente, vencido el cual, de no haber observaciones, se producirá la recepción extintiva de la obra [\[1512\]](#).

4.3.4. Responsabilidad de la empresa (equipo) de programación (contratista)

Evidentemente, el incumplimiento de la entrega de la obra contratada en el plazo pactado hará incurrir en responsabilidad contractual al contratista, salvo que el incumplimiento no le resulte imputable, o se deba a caso fortuito. Un programa que no se desempeñe de acuerdo a las funcionalidades contratadas, pondrá al programador en situación de incumplimiento contractual, sin más. Ahora bien, es posible que el software programado pueda ser entregado, pero le afecten vicios de programación, *bugs*, que no lo hacen estar conforme a lo contratado, según lo pactado en las *Specs*.

Señala Calderón tres hipótesis posibles:

- i) si los defectos de programación hacen impropio al contrato inteligente para los fines tenidos en cuenta al momento de contratarlo;

- ii) si los defectos no tornan impropio al software, pero son ostensibles y el comitente debió haberlos detectado empleando la diligencia en la inspección, pero no lo hizo; y
- iii) los defectos de programación no son ostensibles, están ocultos.

En el primer caso, se aplicará el art. 1273, CCCN, que regula la impropiedad de la obra, que dispone una garantía imperativa que no puede ser dejada de lado convencionalmente. Si bien la norma está evidentemente pensada para la construcción de obras físicas, al hablar de *ruina*, lo cierto es que la *arquitectura* del software permite también trazar una analogía [\[1513\]](#), ya su deficiente diseño y consecuentemente deficiente programación, producirá una equivalencia funcional a la ruina física de una obra: el uso del contrato inteligente no será seguro, y no puede ser afectado al destino que el comitente tuvo en miras al contratarlo.

Ahora bien, no cualquier defecto de programación producirá la impropiedad funcional, ha de ser de una *gravedad* tal que pueda ser determinada pericialmente, y no debe ser posible su subsanación técnica, i.e., una nueva codificación que subsane los vicios detectados. Del mismo modo que esta garantía beneficia a un subadquirente si lo impropio fuera un inmueble, la garantía beneficiará a los sub-usuarios del contrato inteligente afectado, durante todo el plazo legal. De activarse esta garantía, acarreará una responsabilidad objetiva en cabeza del programador, que sólo se podrá liberar si prueba la causa ajena: culpa de la víctima o caso fortuito. Si bien la garantía tiene un plazo de caducidad de 10 años desde recibida la obra, la acción emergente prescribe al año desde que se produjo la causal que produce la impropiedad.

En el segundo caso –defectos de programación que no tornan impropio al software– ante diferencias ostensibles de calidad con lo contratado, la falta de reservas al momento de la recepción liberará al programador, salvo que se haya pactado un plazo convencional de garantía.

En el tercer caso, defectos ocultos de programación, el caso se resuelve como si fuera un supuesto de defectos ocultos que, según su gravedad, pueden ser redhibitorios. Luce poco probable el escenario de defectos ocultos

de programación, ya que usualmente al (mal) programar, los errores de lenguaje se manifiestan rápidamente impidiendo alguna funcionalidad, o dificultando la experiencia del usuario.

4.3.5. Aspectos controvertidos del desarrollo y la comercialización del software

La novel disciplina de los contratos inteligentes presenta muchos aspectos controvertidos, que hacen que el contrato de obra por el cual se contrata el desarrollo y programación de un *Smart Contract* tenga muchas particularidades.

En primer término, la primera pregunta que viene a la mente es si la programación de un contrato inteligente requiere (o no) la participación de un abogado supervisando lo que el código programa, trabajando mano a mano con la empresa de programación [\[1514\]](#). ¿Debieran las normas que rigen el ejercicio profesional del abogado ser modificadas para abordar este nuevo fenómeno? ¿Debiera requerirse un dictamen legal emitido por abogado matriculado? ¿Matriculado dónde?

En segundo lugar, como ya se ha señalado [\[1515\]](#), el software no es *error-free*, y es muy difícil –mas no imposible– garantizar que la programación del contrato no contendrá deficiencias, *bugs*. El caso *TheDAO* ilustra suficientemente el punto. Los errores de programación en materia de contratos inteligentes producen nefastas consecuencias: los fondos asociados al contrato pueden ser robados, destruidos o congelados para siempre [\[1516\]](#), a pesar de existir *buenas prácticas de programación* que permiten evitar algunos errores comunes y conocidos [\[1517\]](#) y que son ampliamente difundidas [\[1518\]](#). Como válvula de escape residual, la programación de un *Smart Contract* debiera siempre dejar a salvo alguna forma de detenerlo, paralizarlo, o hacer un *rollback* [\[1519\]](#).

En tercer lugar, serán cada vez más frecuentes las empresas de tecnología

dedicadas a vender “*Smart Contracts* enlatados”, pre-programados con determinadas funcionalidades, que se comercializan masivamente mediante contratos de licencia, y no se desarrollan a medida mediante contratos de obra. Ejemplos ya abundan: *OpenLaw*^[1520], *Clause*^[1521], *CommonAccord*^[1522], *Agrello*^[1523], y *Legalese*^[1524]. ¿Debería requerirse la participación de abogados en estas empresas?

En cuarto lugar, como ya se ha referido antes^[1525], la traducción del lenguaje natural técnico-legal a lenguaje de programación es una tarea muy desafiante, que difícilmente pueda ser llevada a cabo de manera exitosa sin la colaboración mutua de abogados y programadores. Este riesgo no es menor, y se ha sostenido que:

“the gap between the lawyer’s semantics and the software programmer’s operational semantics may bring unacceptable operational and regulatory risks.”^[1526],

En este sentido, se ha afirmado que:

“Smart Contract programming requires an “economic thinking” perspective that traditional programmers may not have acquired. Indeed, students repeatedly made (a) logical errors that ultimately lead to money leaks, (b) failed to use cryptographic primitives to secure the contracts from attackers, (c) failed to account for the incentives of contract callers, and (d) made errors related to Ethereum (...) [mientras que] a lawyer can neither understand, nor predict the behaviour of, the Smart Contract code, as there is no intermediate language that bridges the gap (...) [y que] **involvement of a lawyer, especially in the heavily-regulated financial industry, in the authoring of contracts, not only Smart Contracts, is paramount.**”^[1527] (el resaltado es mío)

Por tanto, puede afirmarse que el rol del abogado en materia de *Smart Contracts* es bifronte: (i) cuando el *Smart Contract* automatiza una parte de un contrato convencional, el abogado es el único capaz de validar el significado y alcance técnico de cada término jurídico empleado; y (ii) cuando el *Smart Contract* interactúa con algún ámbito regulado, es el abogado quien debe marcar los límites legales que el código del *Smart Contract* debe respetar y, en muchos casos, reflejar [\[1528\]](#).

Lo anterior lleva a concluir que lo adecuado y conveniente será que un contrato inteligente sea producto del trabajo coordinado de programadores y abogados, donde el lenguaje natural técnico jurídico es convertido y traducido a las especificaciones que el programador debe seguir al programar. De este modo, podrá garantizarse que:

“the contract, as written by the lawyer, was correctly translated into code (...) [y, en consecuencia] the operational semantics faithfully represent the denotational semantics and (...)in turn capture the meaning of the legal, business and regulatory semantics. [\[1529\]](#)”

La apuntada necesidad de integrar lenguajes naturales con lenguajes de programación para el diseño eficiente de contratos inteligentes dará derecho al nacimiento de una nueva disciplina, el *Legal Programming*.

En quinto término, también debe tenerse presente que los lenguajes de programación y los compiladores son en sí un producto evolutivo, y muchas veces deben ser reemplazados por fallas de seguridad, tal como ocurrió con Serpent [\[1530\]](#), el lenguaje de programación en Ethereum que precedió a Solidity.

En sexto lugar, cuando se utilizan *Smart Contracts* con formato de licenciamiento *open source*, es frecuente encontrar deslindes de responsabilidad como el siguiente:

“THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, **FITNESS FOR A PARTICULAR PURPOSE** AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS **BE LIABLE** FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF **CONTRACT, TORT** OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE^[1531]”. (el resaltado es mío)

Este tipo de deslinde es muy frecuente, y expresamente libera de responsabilidad al programador por *falta de adecuación para un fin determinado*.

En este sentido, Pablo Palazzi^[1532] analiza la jurisprudencia sobre contratos informáticos de la Cámara Nacional de Apelaciones en lo Comercial, apuntando los casos “Argentoil c/ Soft Pack”^[1533], “Buenos Aires Software”^[1534], “Coca Cola Polar Argentina c/ Soft Center”^[1535], y “Zival’S SA c/ Samia”^[1536].

En el caso “Argentoil” la Cámara Comercial acogió la pretensión de la actora que adquirió un software de gestión, que fue provisto e instalado. Se pactó también la provisión de servicios de soporte y mantenimiento. Como sucede con los paquetes de software a medida, fue necesario que el desarrollador conociera el funcionamiento de la empresa donde se instalaría el software y lo adaptaran a sus necesidades (customización). El proyecto, sin embargo, nunca terminó de ser instalado adecuadamente, lo que originó el litigio. La actora demandó por rescisión de contrato y resarcimiento de los daños y perjuicios que le produjo el incorrecto funcionamiento del software, afirmó haber pagado una suma de dinero por un producto que nunca funcionó debidamente según lo acordado ni se amoldó a los requerimientos y

necesidades del contratante.

Sostuvo la actora que tal situación generó los correspondientes reclamos a la proveedora del software y diversas alternativas que explica (retiro de personal asignado para la implementación del sistema; suspensión del pago de facturaciones; etc.) que condujeron, finalmente, a un intercambio epistolar. Se reclamó a la demandada: i) el reintegro de las sumas que abonara por la compra del software; ii) el reintegro de lo abonado en concepto de analista de sistema y servicios técnicos; iii) el reintegro de lo pagado por la instalación física y lógica de la red (o, en subsidio, el pago de la cantidad necesaria para posibilitar la corrección de sus defectos); iv) el pago de la suma que debió sufragar en concepto de mano de obra adicional para llevar un sistema de contabilidad paralelo; y v) los intereses de las cantidades reclamadas. Las partes encuadraron la relación como una *compraventa*, y la Cámara consideró al contrato como una compraventa.

En el caso “Buenos Aires Software”, la actora contrató un sistema informático de gestión comercial para asuntos contables y administrativos que era “llave en mano”. También se adquirió asistencia técnica. Pese a la existencia de ambos contratos, fue necesario contratar 120 horas adicionales de trabajo de la demandada, pero luego de esta asistencia no se solucionaron los inconvenientes del software en cuestión.

Entonces se reclamó judicialmente el reintegro de lo abonado por el sistema así como el monto pagado en concepto de soporte técnico. En este caso, la Cámara consideró al contrato como una *licencia* de software, y sostuvo: “Los derechos que recaen sobre los mencionados contratos, son de naturaleza totalmente diferente de los relativos a los bienes corporales y, pueden ser cedidos al mismo tiempo a múltiples adquirentes (...). Cabe destacar que la licencia propiamente dicha es una convención por la cual se autoriza a alguien, por un determinado período de tiempo a ejercitar ciertas facultades emergentes de un derecho protegido por las leyes de propiedad intelectual, que permiten al tercero el aprovechamiento económico del bien (...). Sin embargo, el acuerdo que se conoce como “licencia de software” simplemente concede autorización de uso de un programa de computación, excluye expresamente toda facultad que implique explotación y no se da la nota de temporalidad que caracteriza al contrato de licencia conceptualizado

en el párrafo precedente...En consecuencia, y al no transferirse la propiedad o el goce de la cosa no puede hablarse de vicios internos para este tipo de bienes”. La Cámara recoró la existencia de errores en el software, que motivaron la necesidad de su afinamiento, y afirma que las obligaciones del proveedor informático son de resultado y que las mismas estaban incumplidas en el caso concreto.

En el caso “Soft Center”, se había contratado un programa para remuneraciones y recursos humanos. El sistema nunca llegó a funcionar adecuadamente, situación aceptada y reconocida por los técnicos de la demandada quienes infructuosamente durante meses trataron de subsanar los defectos del programa. Se reclamó el monto abonado.

Sostuvo la Cámara Comercial que “Claramente se evidencia ... que estamos en presencia de un contrato de locación de obra. Este convenio ha sido definido como la relación jurídica en virtud de la cual una de las partes - locador- se compromete a ejecutar una obra, material o inmaterial, y la otra - locatario-, a pagar por dicha obra un precio en dinero (...) Y precisamente, una de las notas características de este tipo de contratos es su clasificación como “obligación de resultados”, en franca contraposición a la locación de servicios a la cual se la asimila a una obligación de medios. En la obligación de resultado, el deudor se compromete al cumplimiento de un determinado objetivo, consecuencia o resultado -opus- ..., siendo en el caso concreto, la instalación y puesta en funcionamiento del módulo de remuneraciones del sistema...”.

Finalmente se reitera el estándar aplicable al profesional informático: “...es una sociedad con alto grado de especialización en la materia y que esta conducta resulta incompatible con el profesionalismo que corresponde exigirle en atención a las consecuencias que pueden derivarse de su actuar... Es, en razón de ello, que resulta especialmente exigible una conducta diligente y prudente destinada a prevenir situaciones como la descripta. Cuanto mayor es el deber de obrar con cuidado y previsión, mayor será la obligación que resulta de las consecuencias posibles de los hechos”.

En la visión de Palazzi, se puede extraer la siguiente doctrina judicial de estos cuatro precedentes:

- i) la comercialización de software *a medida* y de un “software *enlatado*” genera siempre una obligación de resultado en cabeza del desarrollador, sosteniéndose que tanto el software como el hardware deben cumplir con la finalidad del contrato, calificando tales obligaciones como de resultado, *que siempre está presente en los contratos informáticos*;
- ii) incluso, la prestación de servicios de mantenimiento puede ser calificada como una obligación de resultado,
- iii) la responsabilidad es objetiva, lo que implica que el proveedor informático tiene la carga de probar *una causa ajena* para eximirse de responsabilidad, y al acreedor le alcanza con demostrar el mero incumplimiento material de lo prometido para que surja una presunción de adecuación causal contra el deudor;
- iv) las cláusulas de limitación convencional de responsabilidad del contrato son plenamente válidas *entre dos empresas*, descartándose en los casos citados la aplicación del Estatuto del Consumidor [\[1537\]](#); y
- v) el software puede ser comercializado mediante de contratos de compraventa, de licencia de software o contratos de obra, en cualquier caso la obligación del proveedor informático es de resultado [\[1538\]](#). Se volverá sobre la licencia de software *infra* en § 4.5.9.

4.4. *Proveedor de servicios de auditoría técnica de Smart Contracts*

Las apuntadas dificultades en la programación de *Smart Contracts* generan un problema que es, en sí, una gran oportunidad de negocio muy importante para ofrecer servicios de auditoría técnica de contratos inteligentes. En alguna medida, se trata de un nuevo tipo de *Due Diligence Legal*, propio del *Legal*

Programming. Empresas que destacan en este campo son *OpenZeppelin* [\[1539\]](#) y *Consensys Diligence* [\[1540\]](#).

En este sentido, el proceso de auditoría de *Smart Contracts* procura detectar errores de diseño, errores de codificación, o vulnerabilidades que hacen inseguro el software por algún otro motivo [\[1541\]](#). El proceso de auditoría normalmente tendrá cinco pasos:

- i) acordar el alcance del servicio de auditoría y revisar las *Specs* de funcionamiento del código a ser auditado;
- ii) hacer testeos controlados al software;
- iii) utilizar herramientas de detección automática de errores de codificación;
- iv) revisión manual del código programado; y
- v) emitir un reporte describiendo las vulnerabilidades detectadas y solucionadas.

4.4.1. Proceso de auditoría

Normalmente, la auditoría inicia con una revisión de la última versión del código ya desarrollado [\[1542\]](#) y a auditar, que debiera ser un reflejo de las *Specs* utilizadas para programarlo. Comitente y contratista deben acordar, necesariamente, cuál versión del software será la auditada, para evitar ulteriores conflictos.

En segundo término, comienzan los testeos del software, funcionalidad por funcionalidad, para comenzar a detectar defectos de programación, si es que existen. Todos los resultados de estos testeos son documentados. En lenguaje de auditor de software, lo usual será testear al menos entre el 75% y el 90% de todas las líneas de programación, lo que se denomina *test line coverage*, lo ideal siendo, evidentemente, llegar al 100% del *script*.

En tercer término, dependiendo del *expertise* y de los recursos de la empresa de auditoría, suele tener lugar una etapa en la cual se utilizan (cada vez más) herramientas de detección automática de *bugs*. Así, se pone al

código *a revisar* al código, y se libera el tiempo de los auditores *Seniors* para enfocarse en problemas más relevantes.

En cuarto lugar, tiene lugar normalmente la revisión manual del código, y es aquí donde los programadores con cierto *Seniority* generalmente se lucen, ya que pueden entender en general cuál fue la intención original plasmada en las *Specs*, y cómo o a dónde en el diseño del software la presencia de un *bug* podría ser problemático, o dónde una funcionalidad, tal como está programada, se aleja de lo previsto en las *Specs*, sin que implique que existen *bugs*.

En cuarto lugar, la información colectada se plasma en un informe o reporte de auditoría [\[1543\]](#), que podrá provocar cambios en la programación para subsanar los defectos encontrados, si los hubiera.

4.4.2. *Productos imperfectos pero perfectibles*

Un estudio del año 2016, señalaba que sobre una auditoría de 16.000 *Smart Contracts* desplegados en Ethereum, el 44% contenía vulnerabilidades en su programación [\[1544\]](#). Así, la auditoría de contratos inteligentes es una técnica por la cual se analiza el código fuente de un *Smart Contract* en busca de errores e inconsistencias, antes de que sea compilado [\[1545\]](#), incluyendo la utilización del contrato inteligente en un simulador, para analizar su respuesta ante distintos escenarios posibles. Se ha sostenido que esta nueva disciplina de la auditoría de contratos inteligentes:

“this new type of due diligence will bring together specialized transactional lawyers who can review the terms of a specific deal, software experts who can analyze Smart Contract program code and its operation on the blockchain, and ‘Smart Contract’ lawyers who can bridge the gap between the two. [\[1546\]](#)„

4.4.3. *El contrato de auditoría técnica de un Smart Contract*

Desde el punto de vista contractual tradicional, el proveedor de servicios de auditoría técnica para contratos inteligentes es un contratista en los términos del art. 1251, CCCN. A diferencia del desarrollador de *Smart Contracts*, que se obliga a una obra intelectual con un resultado eficaz, el proveedor de servicios de auditoría de software provee un servicio, una obligación de hacer que consiste en la realización de cierta actividad, independientemente de su eficacia [\[1547\]](#). Se trata de una obligación de medios [\[1548\]](#), que genera una responsabilidad subjetiva, cumpliéndose el contrato en tanto la actividad se realice de manera diligente. Así, al celebrarse un contrato de auditoría técnica de software, se contrata la realización de una actividad, ésta es *per se* el objeto del contrato. Es en tales actividades que el comitente tiene interés, en función normalmente del alto *expertise* del prestador. La actividad es valorada como fin en sí mismo.

Ahora bien, la línea divisoria entre (i) el servicio de auditoría en tanto fin en sí mismo, y (ii) alguna obra intelectual que permita optimizar la programación de contratos inteligentes, puede ser poco clara. Por ejemplo, imagínese lector la contratación de la confección de una serie de manuales de mejores prácticas de programación, con más unos procedimientos documentados de pasos y formas de revisión y testeado de código, sumado – ahora sí– a la prestación de los servicios de auditoría propiamente dichos. En estos casos, la línea entre la obra y el servicio, será difusa, confusa, profusa. Tanto así, que la distinta naturaleza de las prestaciones del proveedor – asumiendo que fuera el mismo– aconsejaría celebrar dos contratos distintos, uno de obras y otros de servicios.

4.4.4. *Empresa de programación que ofrece servicios de auditoría*

Es posible pensar que la misma empresa dedicada a la programación de contratos inteligentes, pueda ofrecer servicios de auditoría de contratos

inteligentes programados por terceros. En estos casos, evidentemente podría valerse de empleados en relación de dependencia que cumplen una u otra función, según cada cliente. En estos casos, el empleador será *per se* el prestador, de obras o de servicios, de cara al cliente; sus empleados no son proveedores, precisamente por ser empleados del proveedor, y estar regidos por un contrato de trabajo, que tiene su propia regulación legal. Mediando un contrato de trabajo, será el empleador quien asuma ante el comitente los riesgos por las obras o servicios, según el caso, deficientemente prestados.

Desde el punto de vista del comitente, el contratista podrá ser un proveedor en los términos del Estatuto del Consumidor, y generar en consecuencia la aplicación de las normas tuitivas del consumidor a favor del comitente, incluso si fuera una persona jurídica, en tanto se demuestre en el caso concreto el *destino final* del servicio contratado, circunstancia que luce poco probable ya que podría argumentarse fácilmente que el software auditado (i) es utilizado con fines de lucro, o (ii) que existe la intención de obtener un beneficio por su posterior comercialización o (iii) incorporación a un proceso productivo.

4.4.5. Pago al auditor

La forma de retribuir el servicio de auditoría técnica variará en función de la envergadura del trabajo encomendado. El contratista –auditor– podría pactar cobrar sus servicios en dinero de curso legal, o en criptomonedas, o en alguna forma de pago en especie, o en algún porcentaje de los fondos que se transaccionen mediante el contrato auditado, como si fuera un pacto de *Cuota Litis* en los que el Abogado cobra en proporción a la suma cobrada al demandado.

Si el contratista y el comitente no acordaran el precio de la auditoría, el mismo se fija judicialmente de acuerdo a los usos vigentes o al resultado de una pericia.

4.4.6. Prestación de servicios de auditoría y Estatuto del Consumidor

A la prestación de servicios de auditoría técnica le será aplicable el Estatuto del Consumidor si se cumplen los requisitos de proveedor, por un lado, y consumidor o usuario, por el otro. En consecuencia, se aplicarán las normas del consumo previstas en el Capítulo V de la Ley N° 24.240.

Así, conforme al art. 19, “*quienes presten servicios de cualquier naturaleza están obligados a respetar los términos, plazos, condiciones, modalidades, reservas y demás circunstancias conforme a las cuales hayan sido ofrecidos, publicitados o convenidos.*” Se deberá presupuestar la auditoría, de acuerdo a lo previsto en el art. 21, Ley N° 24.240 ^[1549], y será aplicable lo allí dispuesto para la deficiente prestación del servicio ^[1550] y la garantía contractual que el contratista ofrezca al comitente, en los términos del art. 22, Ley N° 24.240:

“Art. 24. Garantía. La garantía sobre un contrato de prestación de servicios deberá documentarse por escrito haciendo constar:

- a) La correcta individualización del trabajo realizado;
- b) El tiempo de vigencia de la garantía, la fecha de iniciación de dicho período y las condiciones de validez de la misma;
- c) La correcta individualización de la persona, empresa o entidad que la hará efectiva.”

4.5. *Proveedor de servicios de Exchange, Trading y Billetera Digital*

Se analizarán ahora las relaciones contractuales que se dan *para ingresar* al ecosistema *blockchain*, y para *permanecer en* y *salir* del mismo.

Salvo el caso excepcional donde alguien es minero de bitcoins y gana *black rewards*, o gana tokens por minería en alguna otra *blockchain*, o los recibe voluntariamente en pago o como donación, el ingreso *voluntario* al entorno *blockchain* normalmente tiene lugar mediante el intercambio de dinero convencional, de curso legal –*fiat currency*, o dinero fiduciario–por monedas digitales, recurriendo al servicio de los *Exchanges*, donde también es posible hacer la operación inversa, es decir, vender criptomonedas a cambio de alguna moneda de curso legal ^[1551].

En alguna medida, los *Exchange* son un tipo de casa de cambio [\[1552\]](#), pero digital, y que no opera con monedas de curso legal, sino virtual. Los *Exchanges* normalmente ofrecen también servicios de intercambio de criptomonedas por otras criptomonedas, es decir, ofrecen servicios de plataforma de *trading*. Una vez que los criptoactivos han sido adquiridos por un usuario, los *Exchanges*, además del *trading*, normalmente ofrecen a sus usuarios los servicios de una billetera digital o *E-Wallet* [\[1553\]](#), aunque éste último servicio se contrata por facilidad y conveniencia, pero no por obligación.

4.5.1. *Exchanges*

El intercambio de moneda convencional por moneda virtual es un sector crecientemente regulado en el mundo, como se analizó más arriba al analizar la legislación de Japón, Francia, Méjico y Corea del Sur, entre otros muchos casos. En Argentina, la situación es también similar, aunque el foco ha sido puesto, por ahora, en el dinero electrónico y las billeteras electrónicas, sin referencia expresa a criptomonedas, como se verá más abajo en § 4.5.13.8.

Luego de los ciberataques a los *Exchange* CoinCheck –que lo llevó a la quiebra en 2018– y a Zaif en el mismo año [\[1554\]](#), el Gobierno Japonés encargó un informe en profundidad a expertos multidisciplinarios sobre las empresas dedicadas a proveer servicios de *intercambio, trading y custodia* de dinero por criptoactivos [\[1555\]](#). El informe recomendó que se exija a los *Exchange* una patrimonio neto mínimo, más la disponibilidad de criptoactivos en reserva para eventuales reembolsos para casos de robo de criptoactivos [\[1556\]](#).

En el mismo año se formó también en Japón la primera asociación empresaria del rubro del mundo, con la finalidad de auto-regular al sector de los proveedores de servicio de *Exchange* [\[1557\]](#).

4.5.2. KYC & AML

En todo el mundo, uno de los puntos más críticos de los *Exchange* es su cumplimiento (o no) de las normas anti-lavado y de financiamiento del terrorismo internacional. En este sentido, existen casos de cierre forzado de *Exchanges* que no cumplían con normas KYC & AML [\[1558\]](#), siendo famosos los casos de cierre forzado de los *Exchanges* BTC-e y World Exchange Services, WEX [\[1559\]](#).

En Argentina, por ejemplo, uno de los más populares *Exchange* es Ripio [\[1560\]](#), cuyos términos y condiciones de uso [\[1561\]](#) expresamente disponen que:

“Toda la información y los Datos Personales ingresados por el Usuario tienen carácter de declaración jurada (...)
CuentaDigital se reserva el derecho de **solicitar comprobantes y/o información adicional** a efectos de corroborar la información entregada por un Usuario en materia de Datos Personales, así como de suspender temporal o definitivamente a aquellos Usuarios cuyos datos no hayan podido ser confirmados. CuentaDigital se reserva el derecho de rechazar una solicitud de registro o de cancelar o suspender, temporal o definitivamente una CuentaDigital (conforme es definida a continuación), en caso de detectar **incongruencias o inconsistencias** en la información provista por un Usuario o en caso de detectar **actividades sospechosas**, sin que tal decisión genere para el Usuario derechos de indemnización o resarcimiento (...) Por razones de seguridad, los Fondos que se acrediten en la Cuenta del Usuario y/o que estén pendientes de liquidación (sin importar el medio de pago por el que se hubiera efectuado la transacción) podrán permanecer indeterminadamente retenidos cuando, a exclusivo criterio de CuentaDigital, **existan fuertes sospechas de ilegalidades, fraude, excesiva cantidad de operaciones o transacciones que**

puedan ser fraudulentas y/o excesivos pedidos de devoluciones y/o contracargos, o cualquier otro acto contrario a estos Términos y Condiciones de Uso y/o **sospechas de violación de preceptos legales** por los cuales CuentaDigital deba responder (...) El Usuario manifiesta que el objeto por el cual se celebra la Solicitud de Procesamiento de Pago no infringe ninguna ley aplicable, ni es por un servicio, venta o transmisión que está prohibida por la ley o los Términos y Condiciones de Uso, tales como y sin limitarse a: (i) juegos de azar, apuestas, etc. que estén vedados por la regulación vigente; (ii) tráfico de armas, de personas, de animales, etc.; (iii) **lavado de dinero y/o terrorismo**; (iv) pornografía, prostitución o pedofilia; y/o (vi) cualquier tipo de actividad que pueda ser considerada fraudulenta o ilegal o sospechosa de serlo (...)

3.2.6. **El Titular no se responsabiliza por el destino de las monedas virtuales que el Usuario adquiere ni es responsable por el origen de las mismos.** En caso de que se solicitara información acerca de la conducta de una cuenta, la misma será provista de acuerdo a lo especificado en el punto 2.2 de estos términos y condiciones.” (los resaltados son míos).

4.5.3. *Monedas virtuales “sospechosas” y listas negras*

El informe japonés ^[1562] también resalta que los *Exchange* tienen la responsabilidad de no tranzar criptomonedas que sean de origen dudoso, y no divulgan adecuadamente su historial de transferencias previas.

En este sentido, una práctica cada vez más usual es difundir “listas negras” de criptomonedas sospechosas, como lo está haciendo la AMF en Francia ^[1563] y FINMA en Suiza ^[1564]. En Suiza solo en 2019 se emitieron 1185 ICOs, de las cuales 30 terminaron con acciones civiles y penales contra los emisores, 10 de las cuales fueron objeto de persecución por violación de normas KYC-AML ^[1565]. En consecuencia, los *Exchange* que apunten a posicionarse seriamente ante sus clientes, debieran no operar criptomonedas incluidas en listas negras.

4.5.4. Relaciones contractuales en el ámbito de los Exchanges

Poniendo foco en la relación contractual existente entre un usuario de criptoactivos y un *Exchange*, se ha señalado [\[1566\]](#) que debe separarse entre (i) los *Exchanges* de criptomonedas que se limitan a ser una plataforma donde las partes directamente entre ellas se ponen de acuerdo en el intercambio de activos digitales *peer-to-peer*; y (ii) aquellas otras plataformas que establecen el valor del activo digital, comprando y vendiendo por cuenta propia, y permitiendo crear *Wallets* en las cuales se puede “cargar” tanto moneda de curso legal como moneda extranjera o incluso criptomonedas, y luego con esos valores se puede realizar pagos de, por ejemplo, servicios públicos [\[1567\]](#).

En el primer caso, la operación de compra o venta de criptoactivos se realiza entre sus dueños –i.e, los poseedores de la llave privada que permite transaccionarlos–, y la plataforma sólo los pone en contacto, con lo que podría calificarse tal funcionalidad del *Exchange* como una *funcionalmente equivalente* a la del contrato de corretaje [\[1568\]](#), cuyo objeto puede ser cualquier cosa, incluyendo bienes inmateriales, y donde el *Exchange* se limita a mediar –a través de una plataforma *on line*–, es decir, a poner en contacto a las partes [\[1569\]](#), que son las que finalmente celebrarán (o no) el contrato de compraventa de criptoactivos. El corredor no representa a las partes [\[1570\]](#), tiene prohibido adquirir para sí los efectos cuya negociación le ha sido encomendada [\[1571\]](#), y su mediación –obligación de medios– le devenga el derecho a una comisión si la operación se termina realizando [\[1572\]](#). Dentro de las obligaciones del corredor [\[1573\]](#), se impone la de verificar la identidad de las personas que intervienen en los negocios que media, y su capacidad legal para contratar. Con relación a la identidad, se sabe que puede ser un punto problemático en entorno *blockchain*. Otra obligación del corredor es la de informar *todas las circunstancias que sean de su conocimiento y que de*

algún modo puedan influir en la conclusión o modalidades del negocio ^[1574]. En materia de criptoactivos, este deber de información debiera incluir mínimas referencias en punto a la volatilidad de los criptoactivos, y a los riesgos asociados a la pérdida de llaves privadas. ^[1575]

Ahora bien, téngase en cuenta que la actividad de intermediación *per se* está regulada por la Ley N° 20.266, del año 1973, en su Capítulo XII y en tan solo cinco artículos, e impone la obligación inderogable del corredor de inscribirse en la matrícula en la jurisdicción donde se actúa ^[1575]. Esta ley especial sigue vigente con la sanción del CCCN, y esta regulación se complementa con otras, que pueden ser aplicables en función del tipo de *bienes* intermediados, y que pueden exigir y delimitar ciertas condiciones *subjetivas* especiales e imperativas para poder operar, tal es el caso del corretaje de títulos valores con oferta pública, específica y profusamente regulado por la CNV ^[1576], o del corretaje inmobiliario regulado en algunas provincias ^[1577].

En el segundo caso señalado, es decir cuando las plataformas establecen el valor del activo digital, comprando y vendiendo por cuenta propia, y permitiendo además crear *Wallets* en las cuales se puede “cargar” tanto moneda de curso legal como moneda extranjera o incluso criptomonedas, el encuadre contractual puede ser más complejo, debiéndose recordar el concepto de contratos conexos antes desarrollado.

En primer lugar, las compras o ventas de criptoactivos por nombre y cuenta propia de la plataforma, serán un típico contrato de compraventa celebrado con el vendedor o comprador, según el caso, del criptoactivo de que se trate. En segundo término, desde el momento en el que el dueño de un criptoactivo voluntariamente lo deje en custodia del *Exchange*, entraremos ya a la órbita de un eventual contrato de depósito o de un eventual contrato de licenciatario de software, que se analiza más abajo en § 4.5.9. En tercer término, cuando el *Exchange* venda por cuenta y orden de su propietario los criptoactivos bajo custodia, serán de aplicación las normas del mandato, de compra o de venta, según el caso. A su vez, estas tres posibles figuras contractuales podrán ser transversalmente atravesadas por el régimen de los

contratos paritarios, por adhesión, o de consumo, según se cumplan o no sus condiciones específicas.

4.5.5. *Ciberataques a los Exchanges: una tendencia preocupante*

Como ya se ha señalado antes, los *Exchanges* en todo el mundo han sido objeto de ciberataques. Sólo en 2018, aproximadamente el 10% de todas las ICOs creadas fueron víctimas de ciberataques [\[1578\]](#), principalmente vía *phishing*.

El más icónico de todos ha sido el que sufrió el *Exchange* japonés *Mt. Gox* en 2014, el mayor a la fecha, de donde se robaron una cantidad de bitcoins que en aquel momento equivalía al 6% de todo el circulante. *Mt. Gox* inició operaciones en 2010, y al momento del ataque, intermediaba el 70% de todas las transacciones de bitcoins, siendo el *Exchange* más grande del mundo [\[1579\]](#). Este *Exchange* sufrió el robo de 850.000 bitcoins, tanto de sus clientes como propios, valuados en 2014 en 450 millones de Dólares [\[1580\]](#), lo que lo llevó a la quiebra.

Otro caso importante fue el robo de 65 millones de Dólares representados en 120.000 bitcoins del *Exchange* Bitfinex en 2016 [\[1581\]](#). Luego en 2018, otro *Exchange* japonés, Coincheck, sufrió el robo de criptomonedas NEM por valor superior a los 500 millones de Dólares [\[1582\]](#). Y en 2019 se vio el triste record de doce hackeos de *Exchanges* [\[1583\]](#), incluyendo el ataque a Uptbit, de dónde se robaron 342.000 Ethers por valor de casi 50 millones de Dólares [\[1584\]](#). Sólo en 2019 se hackeron 510.000 cuentas de usuarios de criptoactivos.

Esta creciente tendencia puede ser consecuencia directa de la falta de una regulación estricta en materia de ciberseguridad, y específicamente, de la deficiente regulación de cómo absorber tales pérdidas. Por ello, el interesante

informe japonés antes citado [\[1585\]](#) ha propuesto:

“It is, however, necessary to take into consideration that SPs have an obligation to customers to return the virtual currency under management and that the face value of non-risk assets may become less than the required amount due to fluctuations in the virtual currency prices. Furthermore, even **if virtual currency under management is leaked, the SP’s obligation to return the virtual currency to the customers is not necessarily exempted. Therefore, it would be appropriate to require SPs to hold assets in the same kind of virtual currency as the funds for reimbursement.**” (el resaltado es mío)

4.5.6. *Litigio colectivo, Exchanges y trading platforms*

A inicios de 2016, en el Estado de Florida, EE.UU se inició una demanda colectiva contra una plataforma de *Exchange, wallet y trading* que operaba bitcoins y otras criptomonedas, llamada *Cryptsy* [\[1586\]](#), inscrita como Money Services Business –i.e., una casa de cambio– en FinCEN, la autoridad de contralor de tales entidades, dependiente del Departamento del Tesoro de EE.UU. Permitía a sus usuarios comprar, vender y *tradedear* criptomonedas.

Luego de que fuera supuestamente *hackeado* en 2014, y perdiera criptoactivos por valor de 5 millones de Dólares, *Cryptsy* continuó igualmente operando, *ocultando* el supuesto ciberataque y la consecuente pérdida a sus clientes y también a FinCEN durante más de 18 meses, y utilizando sus propios fondos para hacer frente a los retiros de criptoactivos a medida que se solicitaban. Durante el proceso judicial, se descubriría posteriormente que en realidad no existió un ciberataque, sino una apropiación indebida y delictiva de los 11.302.961 bitcoins y 13.000 *LiteCoins* de sus clientes por parte de los directivos del *Exchange*, que liquidaron las criptomonedas en otro *Exchange* [\[1587\]](#), y se compraron una mansión en Palm Beach en Marzo de

2015 pagando en efectivo ^[1588]. Ya en Noviembre de 2015, usuarios de Cryptsy empezaron a tener problemas para retirar sus fondos. Dos meses después se inició la demanda colectiva, que fue certificada en Agosto de 2016 ^[1589], y que terminaría revelando la realidad de los hechos y el perjuicio causado y llevando a la quiebra a Cryptsy.

Una acuerdo transaccional con uno de los demandados fue aprobado provisoriamente por el Juzgado en Octubre de 2016 ^[1590], condenándose al otro directivo, aún rebelde, a pagar 8 millones de Dólares en daños y perjuicios ^[1591].

4.5.7. *El caso B2C2 vs. Quoine Pte Ltd.*

Es interesante analizar un caso judicializado en 2019 en Singapur: *B2C2 vs. Quoine Pte Ltd* ^[1592]. El caso involucró a Quoine, un *Exchange* de criptoactivos de Singapur con algoritmos automáticos especializados en *trading* de criptoactivos. Por un error de programación en un algoritmo de *trading* la plataforma de Quoine, se realizaron automáticamente siete operaciones de permuta de Ether y bitcoins, a un precio 250 veces superior al de mercado, beneficiándose a B2C2 quien vio acreditados en su cuenta los montos respectivos, y perjudicándose a otros clientes de la plataforma de Quoine. No hubo ninguna intervención humana en las operaciones. El día siguiente a las operaciones, el CTO de Quoine advirtió el error y revirtió las transacciones. B2C2 demandó a Quoine alegando que la cancelación de las operaciones era una violación del contrato ^[1593] que los vinculaba ^[1594]. La Cámara Internacional de Comercio de Singapur le dio la razón al actor.

Para así fallar, el Juez tuvo en cuenta que de los términos y condiciones del contrato de Quoine, surgía claro que una vez que se acreditaban o debitaban criptoactivos de la cuenta de un cliente, tales operaciones eran irreversibles. Además, consideró que entre las partes se había formado un fideicomiso, siendo Quoine el fiduciario, y el actor el beneficiario, y la acción de reversión de las operaciones llevada a cabo por el fiduciario infringía el fideicomiso,

perjudicando a su beneficiario.

Interesantemente, el juez valoró y rechazó de manera expresa que las operaciones de *trading algorítmico* –luego revertidas manualmente– pudieran ser anulables por un error de programación que beneficiara al dueño del algoritmo, en este caso, el dueño también de la plataforma, Quoine. Se sostuvo:

“The question is not what would have happened if the computer element was absent. **The parties have chosen to use computers as the means of entering the Trading contracts.** They have entered Platform contracts with Quoine so as to be able to enter Trading contracts and, in the case of margin traders, they have entered the Margin trading contracts to regulate their position vis-à-vis the lender, in this case Quoine. **All parties were therefore aware that there was to be no human element in the trades and it is wholly artificial to work on the basis of what might have happened if a human element was involved.**” (el resaltado es mío)

4.5.7.1. El caso Coinzest

En enero de 2019, un *Exchange* surcoreano, Coinzest ^[1595], por error transfirió bitcoins y otras criptomonedas, de manera gratuita y por valor de 5 millones de Dólares, a sus clientes. La transferencia se debió a un error de programación cuando el *Exchange* pretendía realizar un reparto gratuito, un *Airdrop*, de un token, We Game Tokens, como parte de una estrategia de marketing de éstos tokens. Una parte de los clientes del *Exchange* que recibieron por error los bitcoins los devolvieron, pero otra parte los vendió.

4.5.8. Wallets

Analizados los aspectos contractuales y los riesgos inherentes a la actividad

–de momento desregulada en Argentina– de los *Exchanges*, se abordarán ahora las cuestiones contractuales asociadas al uso de billeteras digitales o *Wallets* de criptoactivos.

Repárese sin embargo que se analizará más abajo la nueva regulación argentina de las billeteras digitales para dinero electrónico, aunque debe precisarse que dicha regulación no comprende, por ahora, a las billeteras digitales de criptoactivos. De otro costado, debe tenerse en cuenta que, como se ha visto, es frecuente que los *Exchanges* de criptoactivos ofrezcan también servicios de custodia de los mismos –actúan como *Exchange* y, además, *custodial services provider*–, situación que se corrobora en dos tercios de todos los *Exchanges* ^[1596], por lo cual en tales casos se combinarán las responsabilidades del corretaje con las del –¿quizás?– depósito en una misma empresa, pero existen empresas que se dedican sólo a ofrecer servicios de *Wallet* de criptoactivos, sin operar como *Exchanges*.

En un muy interesante informe del año 2018 preparado por la UNIVERSIDAD DE CAMBRIDGE ^[1597] se sostuvo que las *Wallets* son un *software* que gestiona los pares de llaves públicas y privadas de usuarios de criptoactivos, y en sí, son un intermediario más, que puede presentar riesgos por los usuarios que deciden “tercerizar” la custodia de sus propias llaves. Nótese que el servicio que las *Wallets* ofrecen a sus clientes es el almacenamiento *seguro* de sus llaves privadas, pero no el depósito de los criptoactivos *per se* ^[1598].

Ahora bien, la INTERNATIONAL FINANCE CORPORATION ^[1599] del Banco Mundial sostiene que:

“Despite the high level of security that blockchain systems provide to the data recorded on them, there are some key cybersecurity risks that remain. **The unique challenge to decentralized systems, particularly public blockchains, is that data input can be from any number of nodes, meaning there is a risk of tampering at each node.** The benefit of using a ‘tamper proof’ technology is negated if the information stored on the ledger is compromised to begin with. **This type of attack**

is not aimed at the blockchain itself, but at external systems such as cryptocurrency wallets. There is a risk that individuals might target the data input point (rather than the ledger itself), leading to the dissemination of inaccurate information. Users operating on the blockchain would then unknowingly rely on misleading or false information. Using this approach, it would be possible to **change wallet destinations and amounts of payments. An attacker could divert payments to his own account while making it appear to be the intended destination, ensuring the attack is undetectable to verifying nodes.**” (el resaltado es mío)

En Diciembre de 2018, Saleem Rashid, un niño inglés de tan solo 15 años de edad, detectó una vulnerabilidad en unas de las *Cold Wallets* más utilizada del mundo, el Nano Ledger S [\[1600\]](#), un *hardware wallet* que es un pen drive con algo de software incluido y dos microprocesadores, uno procesa el software de seguridad y encriptación de la *wallet*, y otro procesa la conectividad y una pequeña pantalla. Éste último no era tan seguro, después de todo.

Imagen 13 Nano Ledger S



Rashid no sólo detectó la vulnerabilidad, sino que programó un código de 300 bytes que le permitió ingresar a dos modelos de la *wallet* de Ledger, la *S* y el *blue*, y crear nuevas direcciones –llaves públicas–, con sus respectivas llaves privadas –sólo conocidas por el hacker–, lo que puede permitir cambiar las direcciones de destino y los importes a transferir, sin que el dueño de la *wallet* se de cuenta. Rashid publicó en su blog el hallazgo y notificó a la compañía para que lo resolviese. Sostuvo Rashid:

“Cryptocurrencies, such as Bitcoin, use public key cryptography to protect funds. You can only spend the funds if

you have the private key. This creates an issue for the user as to how they should secure their private key. Humans are notoriously terrible at securing secrets and devices; even security experts are not infallible. To solve this problem, a class of devices called “**hardware wallets**” have been invented. As the name suggests, these are hardware devices that store users’ private keys to protect against malware. Many of these devices connect to a PC via a USB port, but do not reveal the private keys to the PC, much like a hardware security module (HSM). **However, acquiring the private keys is not the only way an attacker can steal your beloved Bitcoin. An attacker who compromises such a device could simply change the recipient of the transaction and the amount being spent! If this is done surreptitiously, many users will be unaware of this attack until it’s far too late to recover the funds.** Therefore, any useable hardware wallet really needs the following features, which differentiate it from a dumb HSM: (i) A trusted display for visual verification of the transaction information; and (ii) On-device buttons, in order to confirm or deny signing transactions. Hardware wallets need to protect against a wide variety of attacks, including: (a) Remote attacks (when an attacker can steal your private keys through malware on your computer) (b) Supply chain attacks (when an attacker can modify the device to do Bad Things before you receive it) (c) Unauthorized physical access (when an attacker can compromise the device if they obtain physical access) ^[1601]” (el resaltado es mío)

4.5.9. *¿Licencia de software o depósito de información?* ^[1602]

Yendo a la naturaleza jurídica del contrato subyacente a la utilización de una *Wallet* ^[1603] de llaves de criptoactivos, debe analizarse si la empresa que

ofrece tales servicios puede (i) ser considerado un depositario de las llaves privadas del propietario de los mismos –identificado con su identidad real y con más sus llaves públicas–; o (ii) es simplemente un licenciante de un software propietario, sin que quepa asimilar al licenciante con el depositario. Las *wallets* ofrecen una experiencia generalmente simplificada de almacenamiento de llaves, que suele atraer a muchos usuarios y, teóricamente, es segura y práctica, aliviando al usuario la gestión de sus llaves privadas. Recuérdese que la pérdida de las llaves privadas equivale a la pérdida de la propiedad del criptoactivo [\[1604\]](#).

En nuestro país, el depósito es un contrato tipificado en los Art. 1356 y 1367, CCCN, que dicen:

“Art. 1356.- Definición. Hay contrato de depósito cuando una parte se obliga a recibir de otra **una cosa** con la obligación de custodiarla y restituirla con sus frutos.

Art. 1367.- Efectos. Si se entrega una cantidad de cosas fungibles, que no se encuentra en saco cerrado, se transmite el dominio de las cosas aunque el depositante no haya autorizado su uso o lo haya prohibido. El depositario debe restituir la misma calidad y cantidad.

Si se entrega una cantidad de cosas fungibles, y el depositario tiene la facultad de servirse de ellas, se aplican las reglas del mutuo.”

Se ha señalado [\[1605\]](#) que en este contrato, cuando es regular, el depositario se obliga a recibir del depositante una cosa para custodiarla y a restituir la misma cosa, con sus frutos. El contrato no transfiere el uso ni el goce de la cosa dada en depósito [\[1606\]](#). Cuando el depósito es irregular, las cosas deben ser fungibles, la transmisión es en propiedad y la restitución debe ser de igual cantidad de cosas, de la misma especie y calidad [\[1607\]](#). Cuando el depósito es regular, el depositario asume una obligación de dar cosas ciertas [\[1608\]](#), y cuando es irregular, de obligaciones de género [\[1609\]](#).

La pregunta que rápidamente surge es si la utilización de una *Wallet* es o puede implicar, efectivamente, la celebración de un contrato de depósito, y en

caso afirmativo, ¿qué tipo de depósito, regular o irregular? La segunda pregunta es cuál es la responsabilidad del depositario de llaves privadas, en caso de sufrir un robo por ciberataque, hartos frecuentes, como se ha demostrado.

Para poder responder la primera pregunta, en función de la regulación actual del contrato de depósito, y de que su objeto sólo puede consistir en cosas, es decir, bienes materiales, muebles o inmuebles, registrables o no [\[1610\]](#), debe antes resolverse si una llave privada es o no es una cosa. En principio, *de lege data*, la respuesta es negativa, con lo cual la figura típica del contrato de depósito no existiría entre el usuario de una *wallet* y ésta, y no tiene entonces mucho sentido analizar la responsabilidad del depositario. En consecuencia, puede sostenerse que existe entre la *Wallet* y su usuario un contrato de licenciamiento de software propietario, que aloja la información relativa a las llaves privadas asociadas a determinadas llaves públicas en una *blockchain*.

Con relación a la licencia de software en general, se ha sostenido que es un contrato previsto expresamente en la Ley N° 25.036, y también en la Ley N° 25.248 de Leasing, por lo que es un contrato nominado, aunque no esté regulado en particular y no tenga un régimen especial aplicable [\[1611\]](#).

Por ello, se sostiene que las licencias de software en su esencia son una *autorización de mero uso o reproducción para ciertos fines*, pero nunca pueden ser asimiladas a una compraventa de la obra, o de los derechos sobre la misma sino a lo sumo solamente del producto físico que la contiene. Una venta de una obra de software (a menos que incluya la cesión de los derechos intelectuales) sólo otorga derecho a *usar* la obra, pero no a *reproducirla* o *copiarla*. En ausencia de otra autorización expresa por el licenciante, éste debe ser el régimen que prime ya que la cesión de derechos no se presume [\[1612\]](#).

En estos contratos de licenciamiento las cláusulas de garantía e indemnidad son muy importantes. Así, se sostiene que el contrato de licencia *debe contener* una garantía de funcionamiento del software licenciado, de acuerdo a algún *service level* mínimo pactado en el contrato, ya que lo contrario implica

desnaturalizar la obligación del proveedor informático ^[1613]. El plazo de esta garantía debe comenzar a correr desde la aceptación de la instalación del software, y es conveniente que se extienda durante el plazo en que se brindan servicios de mantenimiento, los que pueden estar, a su vez, también cubiertos por una garantía contractual (i.e. *Service Level Agreement, SLA*). Como toda garantía contractual, puede contener exclusiones de cobertura, pero deben pactarse expresamente. También debe contener una garantía de evicción sobre la propiedad intelectual ^[1614].

Debe también puntualizarse que Palazzi ha analizado el caso puntual de licencias de software que incluyen componentes de software bajo licenciamiento *open source* ^[1615]. La inclusión de partes de un programa de código informático licenciado bajo alguna de las tantas variantes de licencias abiertas o gratuitas existentes (GPL, OSI, CC, etc.) en un programa de software *propietario* puede traer complicaciones a la hora de determinar las reglas de cada parte respecto a la propiedad del código fuente, las libertades sobre el mismo, usos o destinos, y garantías. Un error común es creer que el *software libre* está en el dominio público, y que por ende se puede incluir *libremente* en cualquier programa propietario sin consecuencia legal alguna, cuando en realidad es justamente lo opuesto: el software libre tiene *autor* y por ende está sujeto al régimen de derecho de autor, de allí que sea posible que éste establezca las libertades o limitaciones que suelen contener esta clase de licencias, con lo cual, será crucial revisar los términos y condiciones de la licencia *open source* de que se trate.

Finalmente, un trabajo muy interesante sobre licenciamiento del software *propietario* es el del Darío Veltani ^[1616]. Afirma Veltani que se trata de un contrato innominado en los términos del Art. 970, CCCN, lo que implica: (i) que al no estar legalmente determinado su contenido, serán las partes las que delimiten su alcance a través de las cláusulas que negocien de manera expresa, aunque frecuentemente se tratará de un contrato adhesivo a cláusulas predispuestas por el licenciante ^[1617]; (ii) adquieren relevancia jurídica los *usos y prácticas* del lugar de celebración; y (iii) se le aplicarán las normas vigentes para contratos nominados *afines* que sean *compatibles* y se adecuen a

su finalidad.

La licencia de uso puede autorizar su uso al licenciatarlo ^[1618], y también en ocasiones su *edición*, con el fin de adaptarlo a *las necesidades del licenciatarlo*, pudiendo el licenciante ^[1619] asumir contractualmente obligaciones de *implementación*, que pueden provocar que el contrato se convierta en un contrato tipificado y nominado de obra ^[1620]. Sus cláusulas usuales son, entre otras, el ámbito territorial de aplicación, el plazo y las condiciones de la licencia otorgada ^[1621], la contraprestación debida al licenciante ^[1622], la descripción del software licenciado ^[1623], el alcance preciso del permiso de uso conferido mediante el contrato de licencia ^[1624] y sus limitaciones ^[1625].

Otra cláusula muy relevante en un contrato de licencia es la de exclusividad ^[1626], así como el mecanismo de recepción y aceptación del software ^[1627]. Con relación a esto último –recepción y aceptación del software–, sostiene Veltani que debido a la posibilidad de que la entrega se realice por canales digitales, en muchos casos su prueba resulta difícil, como también la acreditación de que el software fue aceptado por el usuario.

Así, la recepción del software es el punto de partida necesario para analizar el cumplimiento de las obligaciones de las partes en el contrato de licencia. Además, en el caso del software desarrollado a medida o que ha requerido de algún tipo de adecuación especial para el usuario, también resulta necesario acreditar la aceptación por parte del licenciatarlo, entendida como la confirmación de que el software responde mínimamente a los requerimientos técnicos acordados por las partes.

Con relación a la recepción del software, el contrato de licencia debería regularla teniendo en cuenta el modo en que se distribuirá el software. Si el software se distribuye a través de Internet, podría considerarse como “recibido” por el licenciatarlo en el momento en que ha sido completamente

descargado desde los servidores del licenciante (lo que podría acreditarse mediante el log correspondiente). Pero también constituiría una buena práctica obligar al licenciatarario a realizar un acto positivo, que luego pueda ser acreditado en caso de desconocimiento (por ejemplo, que deba confirmar la recepción del software mediante un correo electrónico o accediendo a un sitio determinado para poder utilizar el software recibido).

Indica Veltani que la jurisprudencia ha dicho que “el suministro de un programa de computación es una conducta más compleja que la carga o imposición electrónica de ese programa en alguna base adecuada para recibirlo. Para suponer dado un programa, en el sentido legal de su tradición al usuario, es menester que éste disponga de los elementos que lo habiliten para emplear el programa”^[1628].

Ahora bine, sostiene Veltani que la *aceptación* es una cuestión más compleja, ya que hay quienes sostienen que “después de la instalación, debería comenzar un período de prueba adecuadamente largo (por ejemplo, 90 días), durante el cual el usuario puede probar el software bajo condiciones operativas reales, en el marco real del usuario y con datos reales”^[1629]. Recién luego de este período de prueba se podría considerar, para esta doctrina, que el software ha sido aceptado.

En este sentido, se ha dicho incluso que debería existir un test de aceptación que debe tener una doble finalidad: (i) en primer término, determinar si el software cumple con las especificaciones comprometidas por el proveedor, desde un punto de vista genérico y abstracto; y (ii) en segundo lugar, si ese software, con los ajustes y adaptaciones correspondientes, funciona bien y cumple los requisitos específicos del licenciatarario, que son los que tuvo en miras al adquirir el software^[1630].

La segunda verificación no tiene ya que ver con el hecho de que el software “funcione bien” sino con que cumpla con las *expectativas específicas del usuario*. Veltani opina que el criterio de rigurosidad del denominado test de aceptación debe variar según sea el tipo de licencia. Es decir, cuando el licenciante ha asumido una obligación de adecuar el software a las necesidades puntuales del licenciatarario, o cuando se trata de una licencia

derivada de un desarrollo a medida o similar, entonces la rigurosidad para evaluar el test de aceptación deberá ser máxima. Pero cuando se trata de una licencia de software estándar, que no requiere de ajustes por parte del licenciante, el test de aceptación podría no incluir el segundo elemento (cumplimiento de las expectativas específicas del licenciatario). En este caso, es fundamental que los términos de la licencia sean claros en cuanto a las especificaciones del software, sus posibilidades y limitaciones, de modo tal que el licenciatario no pueda tener expectativas diferentes. Ahora bien, en caso de que la licencia especifique un test de aceptación, también deberá establecer cuáles serán las consecuencias en caso de que el test falle. En otras palabras, qué pasará si el licenciatario considera que el software no se adecua a los requisitos técnicos y/o no cumple con los requisitos específicos tenidos en miras por el licenciatario al contratar [\[1631\]](#).

Por otro lado, son cláusulas muy usuales de un contrato de licencia aquéllas que regulan las limitaciones de responsabilidad del licenciante [\[1632\]](#), y las que establecen una garantía de funcionamiento del software y de no turbación por parte de terceros [\[1633\]](#).

Dentro de las garantías de funcionamiento del software, se destacan las cláusulas de *Service Level*, que regulan situaciones en las que el software debe ser utilizado en forma ininterrumpida, hipótesis en la que adquieren relevancia los niveles de servicio: es una garantía del licenciante, quien asegura que el software funcionará ininterrumpidamente durante un determinado porcentaje de tiempo, que habitualmente se ubica dentro del 99,9%. Lo esencial de esta cláusula es que en ella se defina adecuadamente: (i) en qué casos se considerará que el software no ha estado funcionando ininterrumpidamente; (ii) cómo se computará el tiempo de interrupción en el funcionamiento; (iii) quién efectuará las mediciones; y (iv) cuál será la consecuencia en caso de verificarse un incumplimiento del tiempo de funcionamiento ininterrumpido garantizado [\[1634\]](#).

4.5.10. *Términos y condiciones de un contrato de licencia*

de Wallet software

Si se acepta el punto de que las *Wallets* no son depositarios, sino licenciantes de un software propietario, será relevante entonces analizar los términos y condiciones de tal contratación. Se tomará como ejemplo –hay cientos– el caso de los términos y condiciones de licenciamiento de una billetera llamada *Hodly* ^[1635]. Puede leerse de los mismos que:

“The Company operates a **software program that enables users to receive, access, store and transfer virtual currencies, tokens, and cryptocurrencies** (collectively, “Cryptocurrency”). This license agreement permits You to use the Wallet subject to certain conditions, rights and obligations (...) The Company **licenses the Wallet to You** on a personal, non-exclusive, royalty-free, non-transferable, worldwide-basis, for the purpose of holding and transferring Cryptocurrencies. **You are not permitted to re-distribute the Wallet, modify any code or use any Wallet content, including images and text, as part of any other software or project of any kind.** You must obtain the Company’s written permission before acting contrary to copyright law or the terms of this clause.” (el resaltado es mío).

En materia de depósitos y retiros, los términos de *Hodly* estipulan:

“You may deposit funds and/or Cryptocurrencies into your Wallet at any time during the duration of your contractual relationship with the Company. **Funds as means of payment for Cryptocurrencies will be accepted via, debit/credit card** (MasterCard, Visa, etc.) supporting the 3D-Secure protocol and Cryptocurrency transfer (BTC, ETH, etc.) **where the originator is you. The Company does not accept third party or anonymous payments in favor of your account.** The Company shall perform withdrawals of your funds and/or Cryptocurrencies, upon an application for withdrawal made via

the Wallet. Upon the Company receiving an instruction from you to withdraw funds and/or Cryptocurrencies from your account, **the Company shall pay/transfer the said amount within one business day**, if the following requirements are met:

a) The withdrawal instruction includes all necessary information;

b) **The instruction is to make a bank transfer to your bank account or digital currency to your blockchain address; and**

c) At the moment of payment, your client account balance exceeds or is equal to the amount specified in the withdrawal instruction including all payment charges.

Withdrawals will only be executed by crediting your personal account. **The Company will not effect withdrawals by transferring the funds to any other third party or to an anonymous account.** The Company reserves the right to decline a withdrawal request when you ask for a specific transfer method and the Company has the right to suggest an alternative. All payment and transfer charges will be borne by you and the Company is entitled to debit your account for these charges.” (el resaltado es mío).

En relación a órdenes judiciales que afecten al usuario de la *Wallet* y sean notificadas a la empresa, los términos y condiciones disponen:

“The Company reserves the right to refuse to process or to cancel any pending Cryptocurrency Transaction as required by law or in response to a subpoena, court order, or other binding government order or to enforce transaction limits. The Company cannot reverse a Cryptocurrency Transaction which has been broadcast to a Digital Currency network. The Wallet services are available only in connection with those Cryptocurrencies that the Company, in its sole discretion, decides to support. The Cryptocurrencies that the Company supports may change from time to time. Under no circumstances should you attempt to use your Wallet to store,

send, request, or receive Cryptocurrencies in any form that are not supported by the Company. The Company assumes no responsibility or liability in connection with any attempt to use the Wallet for Cryptocurrencies that the Company does not support.” (el resaltado es mío).

Y, en materia de liberación de responsabilidad, los términos de licenciamiento naturalmente disponen:

“Using Cryptocurrency-related software necessarily entails many risks. **The Company specifically disclaims and shall have no liability to You for the following risks:** (i) operating system failures (mobile or desktop); (ii) interactions between Your hardware, software and the Wallet; (iii) cloud backup software (e.g. certain Android distributions) may upload your private files/information to third party services; (iv) **malware, viruses or other malicious software on Your device that is able to take control of or interfere with the Wallet;** (v) communication delays between Your Wallet and a node or relay service for a Cryptocurrency (and vice versa); and (vi) **theft of Cryptocurrencies.**” (el resaltado es mío).

A su vez, dado que el uso del software es gratuito, los términos disponen una liberación total de garantías y hasta una obligación de indemnidad *en contra* del usuario:

“The Wallet is provided to You at no cost, “as-is” and **without any warranty whatsoever**, to the maximum extent permissible by law. Without limiting the generality of the foregoing, **the Company does not warrant that the Wallet is fit for Your purpose, even if You have previously provided notice of Your intended purpose, and does not warrant that the Wallet will operate in a bug-free manner.**

You agree to indemnify the Company against any claims, damages, losses or legal fees incurred due to Your use (or

misuse) of the Wallet.” (el resaltado es mío).

Finalmente, en materia de privacidad de la información, los términos y condiciones disponen:

“Your blockchain transactions may be relayed through servers (“nodes”) and **will be publicly visible due to the public nature of distributed ledger systems.**

Exchange rates, balances, transactions and other blockchain information may be read from, or relayed to, third-party servers. We cannot guarantee the privacy of your Internet connection.” (el resaltado es mío).

Evidentemente, muchos términos arriba transcritos colisionan con el Estatuto del Consumidor.

4.5.10.1. El licenciataria de software como usuario protegido por el Estatuto del Consumidor

Siguiendo el razonamiento arriba expuesto de que el usuario de una *Wallet* es, en realidad, un licenciataria de software, la (gran) cuestión que se presenta es si tal usuario es un usuario protegido por las normas de protección del consumidor. El tema excede ampliamente el mero encuadramiento bajo derecho nacional –i.e., Ley N° 24.240 y demás normas–, y se discute actualmente en todo el mundo.

En efecto, en EE.UU, donde la industria del licenciamiento de software es de gran relevancia económica, se ha criticado que los Principios de los Contratos de Software aprobados por el AMERICAN LAW INSTITUTE [\[1636\]](#) infringen las normas de orden público consumeril europeas (y también las Argentinas).

En efecto, en Europa, la protección del software en tanto creación está contenida a nivel comunitario en la Directiva 2009/24/EC, del año 2009 [\[1637\]](#), a la que se le suman la Directiva de Protección de los

Consumidores de 2011^[1638], que reconoce el derecho al desistimiento pero no lo admite en casos de descarga de programas de software vía Internet, típico caso de los contratos electrónicos de tipo *click-wrap*^[1639]; la Directiva de Actos Desleales contra Consumidores, de 2005^[1640]; la Directiva de Comercio Electrónico del año 2000^[1641], que regula los contratos electrónicos^[1642] y la Directiva de Cláusulas Abusivas en Contratos de Consumo, vigente desde el año 1993^[1643].

Respecto a los contratos de licenciamiento, todas las Directivas citadas son de obligado cumplimiento en la Unión Europea, y cada una regula algún aspecto puntual. Así, con relación a cláusulas abusivas en contratos de licenciamiento, la interpretación en caso de ambigüedad será siempre a favor del consumidor, y en un Anexo de la Directiva de Cláusulas Abusivas se encuentran 17 ejemplos de cláusulas abusivas^[1644] que pueden, naturalmente, estar contenidas en un contrato de licenciamiento.

Lógicamente, toda cláusula de limitación de responsabilidad que afecte al usuario final de software licenciado –tal como las vistas en la licencia de *Hodly* en el apartado anterior– será considerada, en Europa y también en Argentina, como una cláusula abusiva y nula, aunque generalmente será operativa y oponible en EE.UU.

Así, la Oficina de Defensa del Consumidor del Reino Unido por ejemplo obligó a Dell Corporation a que modificase sus términos y condiciones de contratación, eliminando cláusulas que limitan la responsabilidad al precio pagado por la licencia o limitan la indemnización de daños y perjuicios por incumplimiento contractual del proveedor, y se concluyó que el típico contrato de licenciamiento *End User License Agreement* –coloquialmente denominado *EULA*– suele contener cláusulas estándar que infringen los derechos de los usuarios bajo el Estatuto del Consumidor^[1645]. Un tribunal francés, por su parte, anuló 31 cláusulas de un contrato de licencia utilizado por el portal América OnLine (AOL), por considerarlas abusivas y violatorias del Estatuto del Consumidor francés, incluyendo la cláusula de limitación de

responsabilidad [\[1646\]](#). También se han anulado judicialmente las cláusulas insertas en contratos de licencia que no permiten al consumidor iniciar una acción judicial y demostrar todos los perjuicios que pueda haber sufrido, o que limitan su derecho a sólo terminar el contrato de licencia [\[1647\]](#).

Ahora bien, si bien desde el punto de vista del derecho de fondo, más específicamente del Estatuto del Consumidor, es innegable que un contrato de licenciamiento de software no esta ni estará *per se* exento de la normativa consumeril en tanto y en cuanto existan un proveedor y un consumidor o usuario *final*, lo cierto y real es que si el proveedor está situado en el extranjero y el contrato de licencia ha sido electrónicamente celebrado, será realmente difícil lograr que el proveedor cumpla la normativa consumeril argentina en sus términos contractuales usados de manera masiva y global vía Internet, y mucho más difícil aún será ejecutar una sentencia que lo condene a indemnizar daños y perjuicios causados por fallas de programación del software licenciado, o incluso por una falla de seguridad que haya permitido, como ha pasado, el robo de llaves privadas en *hot wallets*.

Evidentemente, a mayor tamaño empresarial, es presumible (y esperable) una mayor solvencia patrimonial y una mayor responsabilidad en el cumplimiento de las leyes. Un gran *Exchange* que ofrezca servicios de custodia de llaves probablemente pueda (o no) absorber las pérdidas causadas por una falla de seguridad por la cual se filtren llaves privadas de sus usuarios –como pasó con *Binance* que reembolsó 40 millones de Dólares [\[1648\]](#) en 2019, o *Coincheck* [\[1649\]](#) que reembolsó 435 millones de Dólares en 2018; o, como también ha pasado, quizás se presente en quiebra y deje los perjuicios sin indemnizar.

4.5.11. Hot & Cold Wallets y MultiSig Wallets

Tanto las *hot* como las *cold wallets* tienen algo de software adentro, aunque éstas últimas también incluyan hardware. Las *hot wallets* pueden ser ofrecidas, como ya se dijo, de manera integrada en un *Exchange*, como es el

caso de Coinbase, por ejemplo [\[1650\]](#), on line desde el mismo website del *Exchange*, o en aplicaciones o programas que se instalan en teléfonos celulares o en la computadora del cliente, pero en ambos casos, con conectividad a Internet en todo momento. Estos servicios de *hot wallet* tienen la ventaja de que *permiten recuperar las contraseñas* en caso de olvidarla, a través de preguntas secretas dispuestas por el mismo usuario, como en cualquier servidor de un *home banking* que pide una contraseña para acceder y establece un mecanismo de recupero de la misma.

También hay *Wallets* que imprimen la llave privada en papel, o a través de códigos QR [\[1651\]](#). En las *cold Wallets* [\[1652\]](#), el software se descarga directamente en un pen drive del usuario, o a veces también en su teléfono celular, o también se puede comprar un dispositivo que es *per se* la *Wallet*, y ya viene con el software instalado, como el caso del Nano Ledger S [\[1653\]](#). A su vez, las *hardware cold wallets* pueden ser divididas en aquéllas que sólo almacenan llaves privadas, conocidas como *Hardware Security Model* (HSM), y otras que, además, generan nuevas llaves privadas y además las gestionan para firmar transacciones [\[1654\]](#).

GARTNER, la prestigiosa consultora en Tecnologías, sostiene que la mejor forma de proteger los criptoactivos es usar *cold hardware wallets* y además hacer un copia en papel de las llaves privadas en código QR, y guardar el papel con el código en una caja de seguridad [\[1655\]](#), por si se pierde el pen drive con la *cold wallet*. Las *wallets* descargadas como aplicaciones en teléfonos móviles son fácilmente hackeables.

En efecto, GARTNER afirma con razón que las *Wallets* son el (gran) Talón de Aquiles de *blockchain* [\[1656\]](#). Por supuesto, grandes *Exchanges* pueden ofrecer hasta un seguro para el caso de pérdida de las llaves privadas, como lo hace la plataforma de futuros de criptoactivos *Bakkt*, lanzada por el grupo empresario que controla el New York Stock Exchange (NYSE), y que tiene contratado un seguro de U\$D 125 millones que cubre los bitcoins en ella depositados [\[1657\]](#). Señalan desde GARTNER:

“...most service providers supporting blockchain applications simply retain custody of user private keys, which users often access via password, and **don’t provide any insurance against theft**. This situation concerns those providers because **they then become the single point of failure for their customer’s system access, should they lose control of the private keys**. These worries are justified — this is what played out during breaches of cryptocurrency accounts, where criminals gain control of private keys controlling access to those accounts (...) bad actors can gain access to those data (often crypto assets) by **hijacking centrally maintained private user keys using age-old hacking techniques**. These techniques –for example SIM Swapping or browser session hijacking– have for years helped criminals gain unauthorized access to bank accounts, credit reports, sensitive personal information, intellectual property secrets belonging to private organizations, and pretty much anything they wanted to get their cyber hands on. Hundreds of millions’ dollars’ worth of **crypto assets have been stolen using these very same cyber-bank robbery techniques**. Current implementations of key management —where private keys are centrally maintained— almost negate the benefits of secure cryptographic access that they enable.”^[1658] (el resaltado es mío).

El varias veces referido informe japonés^[1659] recomendó que los *Exchange* que retienen las llaves privadas de sus clientes debieran almacenarlas en billeteras frías, es decir, *off-line* sin conexión a Internet, para evitar robos. Recordar que las *hot wallets* son aquellas que utilizan Internet, sea a través de aplicaciones móviles o desktop, y por tanto están sujetas al riesgo de ciberataque on line. Por ello, en 2018, el 82% de los criptoactivos tenía sus llaves a resguardo en *cold wallets*^[1660].

Recientemente, en relación a los *hot wallets* móviles de dinero electrónico –

i.e., apps que se descargan en el teléfono celular–, el Banco Central de la India ha dispuesto que el proveedor de tales servicios será responsable ante el usuario si éste sufre un ataque por alguna vulnerabilidad tecnológica [\[1661\]](#), reconociéndose al usuario de una *wallet* el mismo derecho a no reconocer una transacción fraudulenta, como si fuera un titular de una tarjeta de crédito que desconoce un débito fraudulento [\[1662\]](#).

También en la India, la Corte Suprema revocó en Marzo de 2020 una circular del Banco Central emitida en Abril de 2020, que le prohibía a los bancos transaccionar en criptoactivos y ofrecer servicios relacionados, en una decisión que sin dudas es un *leading case* a nivel mundial [\[1663\]](#). La Corte Suprema consideró que los criptoactivos no son dinero de curso legal, pero pueden funcionar como unidad de medida, medio de cambio o reserva de valor. La Corte sostuvo que el Banco Central pudo elegir considerar y calificar a los criptoactivos como dinero de curso legal, pero ha decidido no hacerlo, lo que no implica que no tenga capacidad reglamentaria en la materia, la que de hecho, tiene. Sin embargo, se consideró que la actividad reglamentaria volcada en la circular revocada era *desproporcionada*, al no haberse demostrado cuáles son los perjuicios que la transacción con criptoactivos podría causar a los bancos que regula [\[1664\]](#).

Otra forma de proteger las llaves privadas, es utilizar *multi-signature wallets*. Esto permite que para firmar una transacción, deba reunirse una cantidad determinada de llaves privadas. Una sola llave privada no permite firmar transferencias [\[1665\]](#). A fines de 2018, el 87% de las *wallets* ofrecía o utilizaba servicios de *MultiSig* en sus cold wallets [\[1666\]](#).

La prestigiosa AMERICAN BAR ASSOCIATION [\[1667\]](#) ha sostenido en relación al *MultiSig* que:

“Multi-signature transactions illustrate the complexity of application of national laws to cross-border activities. These are transactions that involve more than two parties’ digital

signature approval before settlement can happen. For example, when spending funds come from a bitcoin wallet address, **more than one signature by an applicable private key paired with that wallet address are required before any funds can be spent.** This means that no one individual can transact from this wallet address unless all required digital signatures are obtained. **A typical example is that two out of three digital signatures are required to effect a transaction.** One implication is that the holders of the various keys are legal or natural persons, all resident in differing jurisdictions and providing their signatures from differing jurisdictions. Consequently, governing law in the event of a dispute may be complex and extremely challenging.” (el resaltado es mío).

4.5.12. Ataques a Wallets

Tal como se ha ilustrado con varios casos tristemente célebres, cuando los *Exchanges* ofrecen servicios propios de custodia de las llaves privadas de sus usuarios, asumen el riesgo de ciberataques ya que ofician como un *servidor central on line*, especialmente cuando utilizan *hot wallets*. Sin embargo, se registran también casos de ciberataques a empresas que sólo ofrecen servicios de *wallet*. Los casos más conocidos involucraron a una *wallet* que ofrece un software *MultiSig*, que como se ha visto, es muy utilizado como mecanismo de seguridad *per se* por la ventaja de requerir múltiples llaves privadas para transaccionar criptoactivos.

En el año 2017, la *wallet* Parity [\[1668\]](#) fue dos veces hackeada [\[1669\]](#) en el corto espacio de cuatro meses, sufriendo el robo de distintos criptoactivos valuados en más de 180 millones de Dólares. Luego del primer *hack*, Parity emitió un comunicado de prensa donde dijo:

“On Wednesday 19th July, 2017 **a bug found in the multi-signature wallet** ("multi-sig") code used as part of Parity Wallet software **was exploited** by parties unknown. As of the time of writing, **three wallet accounts holding large balances of ETH**

have been compromised and the balances moved into accounts held by the attacker. To give some perspective: 3 multi-sig wallets were exploited from of a total of 596 vulnerable multi-sig wallets (the rest were commandeered by the White Hat Group), which themselves are a tiny fraction of Parity accounts. The compromised accounts can be viewed on Etherscan. At the time of writing, **the thief is attempting to launder the stolen funds through exchanges.** We already disabled the use of the broken code (it requires use of an on-chain registered resource which we were able to quickly unregister), which means **future multi-sig wallets created in all versions of Parity Wallet have no known exploits.** The bug was in a pair of extremely sensitive functions designed to allow the set-up of "multi-sig" wallets in the Parity Wallet software. The functions should have been protected in order that they be usable only in one specific circumstance, as the contract was being created. However, they were entirely unguarded, which allowed the attacker to reset the ownership and usage parameters of existing wallets arbitrarily. [\[1670\]](#)” (el resultado es mío).

Luego de este primer episodio, la empresa implementó un programa de recompensas para todo aquél que le comunique fallas de seguridad en su software. Se dijo:

“To minimise any potential (technical) security issues the bounty funds will be initially collected into a **cold-wallet account managed by Parity.** This will be transitioned into a multi-sig once we have finalised who the trustees/"owners" of the multi-sig will be that will judge and administer any payments to be made from the fund.” [\[1671\]](#) “Bug Bounty Hunter program rewards are at the sole discretion of Parity Technologies. **The minimum reward for eligible bugs is the equivalent of 100 USD in ETH/BTC.** Rewards over the minimum are at our discretion, but **we will pay significantly more for particularly**

serious issues, i.e. that the identified issue could put a significant number of users at risk of severe damage, monetary or otherwise. Each bug will only be considered for a reward once.”^[1672] (el resaltado es mío).

Cuatro meses después, luego de actualizar y reparar el *bug* del software que permitió el primer hack, la *wallet* de Parity fue nuevamente hackeada, aparentemente por error, pero esta vez sufriendo un impacto económico cinco veces superior, afectándose criptoactivos –Ether– valuados en 150 millones de Dólares. Se dijo desde la empresa:

“Following the fix for the original multi-sig vulnerability that had been exploited on 19th of July (function visibility), **a new version of the Parity Wallet library contract was deployed on 20th of July. Unfortunately, that code contained another vulnerability which was undiscovered at the time** - it was possible to turn the Parity Wallet library contract into a regular multi-sig wallet and become an owner of it by calling the `initWallet` function. It is our current understanding that this vulnerability was triggered accidentally on 6th Nov 2017 02:33:47 PM +UTC and subsequently a user deleted the library-turned-into-wallet, wiping out the library code which in turn rendered all multi-sig contracts unusable and **funds frozen** since their logic (any state-modifying function) was inside the library.”^[1673] (el resaltado es mío).

Respecto de este segundo ataque de Noviembre de 2017, la empresa luego diría que:

“a vulnerability in the “library” Smart Contract code, deployed as a shared component of all Parity multi-sig wallets deployed after July 20th 2017, **was found by an anonymous user. The user decided to exploit this vulnerability and made himself**

the “owner” of the library contract. Subsequently, the user destructed this component. Since Parity multi-signature wallets depend on this component, this action blocked funds in 587 wallets holding a total amount of 513,774.16 Ether as well as additional tokens.” (el resaltado es mío).

Los fondos afectados –más de 500.000 Ether– nunca pudieron ser recuperados, ya que la única forma de retrotraer la operación hubiera sido un *hard fork* en Ethereum, que fue propuesto a la comunidad de nodos de Ethereum, pero fue rechazado [\[1674\]](#). Es más, las cosas luego no mejoraron mucho para esta *wallet*, ya que un informe de auditoría del código de su *wallet MultSig* de Mayo de 2019 afirmaba que casi un 40% de sus nodos no había actualizado el software con correcciones de *bugs* desarrollado dos meses antes, con lo cual estaban expuestos a serios ciberataques [\[1675\]](#). La empresa había pedido en Febrero de 2019:

“It has come to our attention that **the scope of the fixed Parity Ethereum vulnerability is wider than we originally thought**, and it could be exploited from a regular node-to-node connection without RPC access. While the previously released 2.2.10-stable and 2.3.3-beta protect against this wider scope, the wider scope means that **everyone** who runs Parity Ethereum, not just those who serve JSON-RPC publicly, **should update as soon as possible**. The 2.2.10-stable and 2.3.3-beta releases protect Parity Ethereum nodes from potentially being able to be crashed by a targeted attack.” [\[1676\]](#) (el resaltado es mío).

Evidentemente, la *blockchain* como tecnología puede ser y es muy segura y ofrece una ciberresiliencia única, pero es innegable que los *puntos de acceso* a ella no son tan seguros, como se ha demostrado con los ataques a *Exchanges* y *Wallets*, y los puntos de acceso son y seguirán siendo el objeto de ciberataques muy sofisticados, y muy difícilmente penados, ya que sus autores son difícilmente rastreables, y pueden estar operando desde cualquier lugar del

mundo.

En este sentido, se ha sostenido que existen al menos *diez* formas de hackear a un usuario de criptoactivos [\[1677\]](#): (1) si se utilizan *hot wallets*, que están conectadas a Internet, sea en versión *mobile* o *desktop*, el software de las billeteras puede ser hackeado y se pueden robar las llaves privadas que alojan, perdiéndose para siempre la disponibilidad de los criptoactivos involucrados, e incluso, pudiéndose atacar también a algunas *cold wallets*, como demostró Saleem Rashid; (2) *e-mail phishing* que engañan al usuario, quien introduce sus claves y cae en la trampa; (3) *keyloggers*, es una especie de *malware* que almacena toda información que parezca una clave, y la transmite a un tercero. Estos *malwares* pueden infectar computadoras al descargarse archivos adjuntos en un e-mail sin chequeo de antivirs, o al descargar software online de sitios inseguros, o incluso al conectar un pen drive infectado; (4) *wallets* falsas, que se parecen a *wallets* serias, pero en realidad son una simulación que a veces pueden ser descargadas de App Stores muy conocidos; (5) falsos representantes de *Exchanges* o de emisores de tokens, que engañan a los usuarios y los convencen de que transfieran tokens a una determinada dirección, que controla un hacker; (6) troyanos, que detectan claves de criptoactivos y las transmiten a terceros, de modo similar a un *keylogger*, (7) extensiones de navegadores de Internet que almacenan datos que parecen contraseñas y los transmiten, camuflando la descarga como una actualización del software del navegador; (8) violando las medidas de seguridad de doble factor, cuando están disponibles; (9) campañas de publicidad falsas que invitan a la compra de criptoactivos, que pueden hacer creer a un usuario que, al transferir sus criptoactivos a una dirección determinada en forma de pago, recibirá luego los tokens que “compró”, pero en realidad, ha sido víctima del conocido “Cuento del Tío” versión 2.0; y (10) falsificando llaves públicas de una empresa: cuando un comercio acepta como pago criptoactivos, normalmente informa a sus clientes cuál es su llave pública en su website, pero existen malwares que, de manera inadvertida, modifican esa dirección al momento de cargarse en la *wallet*, y producen que la transferencia de criptoactivos sea “desviada” hacia otra cuenta: a la del creador del malware [\[1678\]](#).

4.5.13. La regulación argentina de las billeteras digitales. Los Proveedores de Servicios de Pago y el Dinero electrónico

El informe japonés ya citado puntualizaba que, tanto respecto del dinero electrónico como de las criptomonedas, las billeteras digitales japonesas –los prestadores de servicio de procesamiento de pagos–, tienen la obligación de mantener los fondos de sus clientes depositados en una cuenta bancaria separada de sus fondos propios [\[1679\]](#), a los fines de evitar la confusión patrimonial en caso de insolvencia.

Si bien en Argentina se ha regulado de manera puntual y muy específica a algunos aspectos de los procesadores de servicios de pagos, como se verá en el apartado siguiente, se ha sostenido con razón que los sistemas electrónicos de pago carecen de una *regulación general*.

En este sentido, reputada doctrina separa los sistemas electrónicos de pagos entre: (i) sistemas electrónicos de prepago; (ii) sistemas electrónicos de pago instantáneo; y (iii) sistemas electrónicos de pospago [\[1680\]](#). En los primeros –*prepago*–, es necesario que el usuario remita una suma de dinero al proveedor del servicio con carácter previo a usar los fondos; en los segundos –*pago instantáneo*– la entrega del dinero se hace al momento de comunicar la instrucción de pago y en los terceros –*pospago*– la entrega de los fondos es posterior a la comunicación y la ejecución de la instrucción de pago [\[1681\]](#).

La doctrina indica que dentro de los sistemas de prepago, se ubican también los sistemas de *dinero electrónico*, cuyo funcionamiento es muy similar al de los PSPs que se verán más abajo. Si bien no existe en Argentina, a Abril de 2020, una regulación específica del *dinero electrónico* como sí ocurre en la Unión Europea [\[1682\]](#), sí tenemos más desarrollo regulatorio en los sistemas de pospago, con la Ley N° 25.065 de Tarjeta de Crédito.

Chomczyk define al *dinero electrónico* como todo valor monetario almacenado por medios electrónicos o magnéticos que representa *un crédito contra el emisor*, se emite al recibo de fondos con el propósito de efectuar operaciones de pago y que *es aceptado por una persona física o jurídica*

distinta del emisor de dinero electrónico. Lo propio y distintivo del dinero electrónico es la entrega de fondos y su disponibilidad en una plataforma mantenida por el emisor del dinero electrónico. Por tanto, el dinero electrónico es un instrumento de pre-pago [\[1683\]](#), caracterizado por la precedencia lógica de un contrato de depósito irregular por parte del titular de los fondos, celebrado con el emisor del dinero electrónico [\[1684\]](#).

Afirma Chomczyk que el hecho de que exista una *entrega de fondos al emisor de dinero electrónico* –como parecería ser el caso de los PSPs de acuerdo a la regulación que se analiza *infra*– hace pensar que *los PSPs son emisores de dinero electrónico*, sin perjuicio de su interacción en el sistema de pagos minoristas.

Ahora bien, precisa el autor citado con mucha razón que es competencia exclusiva y excluyente del Honorable Congreso de la Nación regular el dinero electrónico, pudiendo el BCRA sólo reglamentarlo [\[1685\]](#), con lo cual es dudoso que el BCRA pueda, en ausencia de una Ley del Congreso, determinar por una comunicación dónde corresponde reservarlos o cómo se los puede aplicar. Así, se ha puntualizado que el BCRA tiene facultades, conforme al art. 47, inc. f), de la Carta Orgánica del BCRA para reglamentar los *sistemas de dinero electrónico*, pero no hay normativa general a partir de la cual se pueda dictar esa reglamentación que la misma Carta Orgánica del BCRA señala como un paso necesario *preexistente* al dictado de la reglamentación. Señala Chomczyk que dado que el texto de la regulación sobre PSPs podría entenderse como una extralimitación del BCRA en sus facultades, habría optado por encarar el tratamiento bajo la noción de sistemas de pagos, donde el BCRA sí tiene plena autoridad. Sin embargo, al determinar cómo debe ser la relación entre el PSP y los fondos del cliente, elemento central de los sistemas de dinero electrónico, la legalidad de ciertas secciones de la norma reglamentaria podría ser cuestionada.

Se analiza a continuación la nueva regulación vigente desde Marzo de 2020 sobre el vertical de *pagos* del ecosistema Fintech argentino, el segundo vertical más importante del ecosistema [\[1686\]](#).

4.5.13.1. El auge de los procesadores de servicios de pago

El Banco Central de la República Argentina (BCRA) tiene el poder de policía para regular no sólo los servicios y a las entidades financieras, sino también los *servicios complementarios de la actividad financiera y servicios permitidos* [\[1687\]](#).

Así, el BCRA recientemente ha regulado a los Proveedores de Servicios de Pago (PSPs), es decir, a aquellas personas jurídicas que prestan servicios relacionados con el procesamiento de transacciones de pagos y/o cobros mediante la utilización de distintos medios de pago, tales como tarjetas de débito, tarjetas de crédito, tarjetas prepagas, plataformas de pagos móviles (PPM) y otros medios electrónicos de pago [\[1688\]](#).

Es importante tener presente la tendencia de crecimiento de los PSPs. Se ha señalado que entre el primer semestre de 2018 y el primer semestre de 2019, el volumen de transacciones minoristas a través de PSPs –i.e, tarjetas prepagas y billeteras digitales– crecieron un 74% y el 279%, para las transacciones con tarjeta prepagas y entre cuentas de pago pertenecientes a las billeteras electrónicas, respectivamente, representando a 2019 el 2,22% del total de pagos minoristas [\[1689\]](#).

Los PSP son personas jurídicas que, sin ser entidades financieras, cumplen al menos una función dentro de un esquema de *pago minorista*, en el marco global del sistema de pagos. Los pagos minoristas incluyen las transferencias de fondos o pagos de alto y bajo valor, con la excepción de los pagos de entidades financieras entre sí y con el BCRA, que son consideradas mayoristas [\[1690\]](#).

Entiende el BCRA que los esquemas de pago son sistemas de reglas comerciales, técnicas y/o operativas que hacen posible las transferencias de fondos o pagos en los que intervienen tres partes: un ordenante, un receptor, y uno o más PSPs. Un medio de pago puede tener uno o más esquemas de pago alternativos. Todo esquema de pago debe tener un administrador que define estas reglas y es el responsable de su adecuación al marco legal y normativo

vigente.

No se consideran esquemas de pago minoristas a los fines de las Comunicaciones “A” 6154 del 13 de Enero de 2017 y “A” 6885 del 30 de Enero de 2020 que los regulan, a: (i) los esquemas de pago regulados por la Comisión Nacional de Valores para la colocación primaria y/o negociación secundaria, y/o la compensación y/o liquidación de valores; y (ii) los esquemas de pago cuyo objeto sea la retención y/o percepción y liquidación de sumas destinadas a cancelar obligaciones tributarias o de otro orden con el Estado en cualquiera de sus niveles y agencias.

La Com. “A” 6885 dispone que no pueden operar como PSPs: (i) las personas jurídicas que no se encuentren regularmente constituidas en el país, o que, siendo personas jurídicas privadas constituidas en el extranjero, no hayan dado cumplimiento a lo requerido en la Ley General de Sociedades para el ejercicio habitual de actos comprendidos en su objeto social; (ii) las personas jurídicas que las normas de la Comisión Nacional de Valores reconozcan expresamente como Mercados, Cámaras Compensadoras, o Agentes de cualquier tipo; y (iii) las personas jurídicas cuyo capital, derechos de voto, órganos de administración o fiscalización estén integrados por personas comprendidas en lo previsto en los incisos a), b), d), e) o f) del artículo 10 de la Ley de Entidades Financieras [\[1691\]](#), o que registren condena por delitos dolosos contra la propiedad, la administración pública, el orden económico y financiero, o la fe pública; por violación de secretos y de la privacidad, asociación ilícita, o por infracción al artículo 1° inciso b) del Régimen Penal Cambiario, excepto respecto de las participaciones accionarias adquiridas en mercados de valores que no alcancen el umbral del 20% del capital o derechos de voto [\[1692\]](#).

El universo de los PSPs adquirió relevancia, utilidad y mucho protagonismo recientemente, cuando el BCRA creó la *Clave Virtual Uniforme* (CVU). El CVU permite la identificación y trazabilidad de transferencias de fondos que se realicen entre cuentas a la vista cuando, como mínimo, una de ellas pertenezca a un PSP, lo que a su vez habilitó la *interoperabilidad* entre cuentas a la vista y servicios de pago [\[1693\]](#). Por otro lado, el CVU permite

que aquellas personas (incluyendo comercios) que no tienen una cuenta bancaria pero sí son clientes de un PSP, puedan recibir o hacer pagos electrónicos desde/a personas con cuenta bancaria.

Este fue un paso realmente muy trascendente, catapultando al sector *Fintech* argentino, al ser probablemente el primer país del mundo en admitir esta interoperabilidad entre billeteras digitales entre sí (cuentas no bancarias) y con cuentas bancarias, posibilitando transferencias inmediatas entre el sector bancario y el sector no bancario [\[1694\]](#).

4.5.13.2. *El fenómeno Mercado Pago*

Con el CVU permitiendo realizar cobros digitales al margen del sistema bancario, muchos comercios argentinos vieron una oportunidad para, a la vez, (i) facilitar la experiencia de compra a sus clientes, admitiendo el cobro y pago mediante billeteras digitales no bancarias, y (ii) invertir transitoriamente la liquidez así obtenida en fondos comunes de bajo riesgo.

Por el volumen de transacciones de ciertos PSPs al transaccionar miles de pagos diarios, esta oportunidad de una inversión transitoria y *click-through* resultó ser disruptiva por el volumen captado y por ser tan inclusiva. En efecto, en solo un año, la billetera digital de Mercado Libre (Mercado Pago) captó más de un millón de cuentas comitentes, abriéndose entre dos mil y tres mil cuentas por día, para realizar inversiones en un monto promedio inferior a los 100 USD [\[1695\]](#), capturando dos tercios del mercado de cuentas comitentes argentinas y administrando un fondo de aproximadamente 110 Millones de Dólares [\[1696\]](#).

Ahora bien, debe resaltarse que las PSPs recurrieron a la *inversión transitoria* en fondos comunes de inversión del tipo “*money market*” *por defecto*. En efecto, de los términos y condiciones de Mercado Pago podía leerse, antes del dictado de la Comunicación “A” 6885 del 30 de Enero de 2020, que el cliente daba la orden de invertir los saldos disponibles en la cuenta de Mercado Pago en cuotapartes de Mercado Fondo [\[1697\]](#), sin que se cobren comisiones por suscripción o rescate, y autorizaban a Mercado Pago a

que los saldos futuros disponibles de una Cuenta Mercado Pago *sean automáticamente invertidos*, aceptándose que los débitos que le correspondan por compras u otros conceptos vinculados a su carácter de usuario de Mercado Libre o Mercado Pago, importarán una instrucción de rescate de Cuotapartes del Fondo.

El cliente del PSP puede decidir utilizar parcial o totalmente sus Cuotapartes para cancelar pagos por la compra de bienes, productos o servicios adquiridos a través de plataformas de terceros, o realizar envíos de dinero a otros usuarios de las plataformas, *o retirar el dinero que compone la inversión en Cuotapartes para su depósito en una cuenta bancaria*, lo que implica una instrucción de rescate.

4.5.13.3. La Comunicación “A” 6859

En tal escenario de auge de las PSPs, y de fuerte crecimiento de los servicios accesorios a las billeteras digitales como de las cuentas comitente para invertir *por defecto* los saldos disponibles en la billetera digital, es que llegó, primero, la Comunicación “A” 6859 de fecha 09/01/2020 [\[1698\]](#).

La Comunicación en estudio cambió el orden de las cosas, al disponer que “el 100 % de los fondos de los clientes deberá encontrarse depositado –en todo momento– **en cuentas a la vista en pesos en entidades financieras del país...**Sin perjuicio de ello, **ante solicitud expresa del cliente**, los saldos acreditados en cuentas de pago **podrán ser transferidos** para su aplicación a la realización de operaciones con “fondos comunes de dinero” [\[1699\]](#) en el país, debiéndose debitar la cuenta de pago. En este último caso, **se requerirá que los saldos invertidos sean informados de manera separada del resto.**” (el resaltado es mío).

En consecuencia, a partir de la entrada en vigencia de la Comunicación en cuestión el día 31 de Enero de 2020, y salvo *expresa decisión* de un cliente de PSP de invertir [\[1700\]](#) sus saldos disponibles suscribiendo cuotas partes, ahora los saldos deben forzosamente ingresar al sector bancario, soportar comisiones bancarias, pagar el impuesto al débito y crédito bancario, y

depositarse en cuentas corrientes a la vista en Pesos, que son remuneradas conforme acuerden las partes [\[1701\]](#), pero que tienen un rendimiento sensiblemente inferior al de los fondos de money market.

4.5.13.4. La Comunicación “A” 6885

Al poco tiempo del dictado de la Com. “A” 6859, el BCRA siguió avanzando en la regulación del Ecosistema *Fintech*, dictando la Com. “A” 6885 [\[1702\]](#) por medio de la cual se regula a los PSP que ofrezcan cuentas de pago, las que son definidas como “*cuentas de libre disponibilidad ofrecidas por un PSP a sus clientes para ordenar y/o recibir pagos.*”

La Com. “A” 6885 dispone, por un lado, que los PSP que ofrecen cuentas de pago deben inscribirse en el “Registro de proveedores de servicios de pago que ofrecen cuentas de pago” habilitado por la Superintendencia de Entidades Financieras y Cambiarias (SEFyC) [\[1703\]](#). Satisfecha la inscripción, la SEFyC emite un certificado de inscripción y otorgará al solicitante un número en el “Registro de proveedores de servicios de pago que ofrecen cuentas de pago”.

La Com. “A” 6885 dispone, por otro lado, que los PSP deben cumplir un régimen informativo y de vigilancia, debiendo dar acceso a sus instalaciones y documentación al personal de la SEFyC designado al efecto, y poner a disposición del BCRA las herramientas de consulta en tiempo real y reporte que la Subgerencia General de Medios de Pago determine para cada tipo de proveedor y según su volumen de operaciones [\[1704\]](#).

Por otro lado, la Com. “A” 6885 también obliga a los PSPs a que en toda publicidad efectuada a través de cualquier medio y en toda documentación emitida por un PSP se incluya una mención clara y expresa de que: (i) se limitan a ofrecer servicios de pago y no se encuentran autorizados a operar como entidades financieras por el Banco Central de la República Argentina; y (ii) *los fondos depositados en cuentas de pago no constituyen depósitos en una entidad financiera, ni cuentan con ninguna de las garantías que tales depósitos puedan gozar de acuerdo con la legislación y reglamentación aplicables en materia de depósitos en entidades financieras.*

Debe también resaltarse lo previsto en el apartado 3.3.1 de la Comunicación bajo estudio, cuando dispone:

“Para la realización de transacciones por cuenta propia (pago de proveedores, pago de sueldos, etc.), los PSPs deberán utilizar una cuenta a la vista “operativa” (de libre disponibilidad) distinta a la cuenta donde se encuentren depositados los fondos de los clientes.”

Esta exigencia, junto con la impuesta por la precedente Com. “A” 6859 que obligó a depositar el 100 % de los fondos de los clientes en todo momento en cuentas a la vista en pesos en entidades financieras del país, apuntan a minimizar el riesgo de insolvencia del PSP^[1705], separando los fondos propios del PSP en una cuenta bancaria *distinta* a la cuenta donde se encuentran depositados los fondos de sus clientes, de modo tal que éstos no sufran riesgo de eventual embargo por los acreedores del PSP^[1706].

Cualquier incumplimiento de los PSPs a lo reglado en ambas comunicaciones glosadas, tornará procedentes las sanciones previstas en los Artículos 41^[1707] y 42^[1708] de la Ley de Entidades Financieras y disposiciones concordantes respecto de los miembros de sus órganos de gobierno, administración y fiscalización.

4.5.13.5. *El ecosistema Fintech argentino*

Estudios recientes del sector Fintech argentino indican que operan en el sector 133 firmas, de las cuales el 80% tiene menos de 50 empleados, ocupando el tercer lugar en el ecosistema Fintech latinoamericano, detrás de Méjico y Brasil^[1709].

El sector brinda una gama de servicios que incluye crowdfunding, *Insuretech*, pagos y transferencias, inversiones, *blockchain* & crypto, servicios fintech B2B, seguridad informática y préstamos^[1710], y genera ingresos a

través de cinco modelos de ingresos predominantes: honorarios de licenciamiento y otros servicios digitales (17% sobre el total), intereses por financiamiento (13%), honorarios y comisiones de *brokering/trading* (12%), honorarios por soluciones *as-a-service* (25%) y comisiones por uso de plataforma tipo e-commerce y/o marketplace (33%) [\[1711\]](#).

Luego de las Fintechs dedicadas a otorgar préstamos -la categoría más desarrollada donde sobresale Afluenta [\[1712\]](#)-, se destacan las Fintechs que ofrecen servicios de pagos y transferencias, entre los que destaca la billetera virtual, una herramienta de pago digital para enviar y recibir dinero, pagar servicios y realizar compras en comercios y en páginas web [\[1713\]](#). Los clientes de estas Fintechs no requieren una cuenta bancaria para operar, y esto es un dato importante toda vez que en 2017 sólo el 49% de la población adulta argentina poseía una cuenta bancaria [\[1714\]](#), y a Marzo de 2019 el acceso al crédito en el sistema financiero alcanzó sólo al 51% de la población adulta [\[1715\]](#).

4.5.13.6. Marcos regulatorios de los ecosistemas Fintech: el proyecto de SandBox español

No existe consenso entre los gobiernos sobre cómo regular la industria de las Fintech, debido a que la industria se encuentra en plena etapa de crecimiento y a que la naturaleza del sector implica debates largos, con participación de múltiples instituciones y empresas, cada una con sus propios intereses. Sin embargo, la regulación emergería como una herramienta clave para dinamizar la industria mediante la financiación, *ya que ofrece reglas claras y establece las bases para el desarrollo del ecosistema* [\[1716\]](#).

En nuestro país, la regulación sobre la prestación de los servicios financieros se concentra en tres entes: el Banco Central de la República Argentina (BCRA), la Comisión Nacional de Valores (CNV) y la Superintendencia de Seguros de la Nación (SSN). De acuerdo a las categorías del mercado Fintech, todas caen dentro de la regulación del BCRA,

independientemente de su actividad, pero las Insuretech, además, son reguladas por la SSN, y las que compongan fideicomisos o participen de inversiones, por la CNV [\[1717\]](#).

En Julio de 2018, el Ministerio de Economía y Empresa del Reino de España presentó un Anteproyecto de ley de medidas para la Transformación Digital del Sistema Financiero [\[1718\]](#), abriendo el debate en España para la creación de un *Fintech SandBox*, es decir, un espacio controlado al estilo inglés, para probar nuevos modelos de negocios centrados en la innovación financiera, con el potencial de generar 5.000 empleos más en los próximos dos años y atraer 1.000 millones de Euros adicionales de inversión [\[1719\]](#).

El Proyecto de ley español aspira a sentar las bases para crear un entorno seguro en el que puedan probarse innovaciones tecnológicas en el ámbito financiero *antes de su comercialización*, bajo estricto seguimiento de los supervisores y con máximas garantías para los participantes. Se concibe principalmente como un instrumento que facilitará la adaptación al proceso de transformación digital tanto de los actores públicos, como de los privados. En particular será un instrumento para mejorar la supervisión y también para acompasar la legislación financiera con la transformación digital [\[1720\]](#).

En este sentido, el acceso al *SandBox* no supondrá en ningún caso autorización para el comienzo del ejercicio de una actividad o para la prestación de servicios de carácter profesional habitual, por lo que los proyectos piloto y las pruebas propuestas dentro de tales proyectos no se encontrarán sujetas a la legislación específica aplicable a la prestación habitual de servicios financieros, debiendo cumplir, en todo caso, con lo dispuesto en esta ley y en el correspondiente protocolo. A su turno, el acceso al *SandBox* requiere garantizar tres ámbitos especialmente sensibles: la protección de datos de carácter personal, la protección a los usuarios de servicios financieros y la prevención del blanqueo de capitales y la financiación del terrorismo [\[1721\]](#).

El Proyecto regula el régimen de acceso al *SandBox*, el régimen de garantías

mientras se desarrollan los proyectos y se celebran las pruebas ^[1722], y, finalmente, y el régimen de salida y los efectos posteriores a la finalización de dichas pruebas, resaltándose en esta etapa una *reducción sustancial de trámites en caso de que no existiese hasta el momento licencia para la actividad*, en aquellos supuestos en los que la actividad para la que se requiera autorización se pretenda realizar principalmente a través de la tecnología y un modelo de negocio *probados*, y los supervisores estimen que la realización de pruebas permite un análisis simplificado del cumplimiento de los requisitos para dicha autorización ^[1723].

De convertirse en ley, el Proyecto en cuestión establecerá la aplicación del *principio de proporcionalidad* ^[1724] entre actividades y riesgos en el ámbito financiero, que garantice que los requisitos exigidos sean proporcionales a los riesgos asociados a cada actividad, *asegurando la igualdad de trato a todas las entidades*.

4.5.13.7. Hacia el Open Banking

Se ha señalado ^[1725] que la Unión Europea asumió una postura de regulación activa respecto de los PSP con la aprobación de la *Payment Services Directive 2* (conocida como *PSD2*) en noviembre de 2015.

La *PSD2* impone un régimen de autorización previa para operar como PSP, dejando que cada país miembro de la UE pueda eximir de dicho requisito a entidades que no alcancen cierto volumen mínimo de operaciones (aunque siempre deben llevar al menos un registro de ellas). La *PSD2* incluye, para los PSP autorizados y como condición para mantener dicha autorización, requisitos de capitales mínimos, de efectivo mínimo e inclusive de la contratación de seguros de responsabilidad civil. Los requisitos varían en su cuantía dependiendo de la cantidad de actividades que el PSP pretenda realizar. La *PSD2* también establece que “*los fondos [de los PSP] no se mezclarán en ningún momento con los fondos de ninguna persona física o jurídica que no sean los usuarios de servicios de pago en cuyo nombre se dispone de los fondos y, en caso de que todavía estén en posesión de la entidad*

de pago y aún no se hayan entregado al beneficiario o transferido a otro proveedor de servicios de pago al final del día hábil siguiente al día en que se recibieron los fondos, se depositarán en una cuenta separada en una entidad de crédito". Sin embargo, en el caso de la PSD2 se posibilita que estos fondos se inviertan momentáneamente en "*activos seguros, líquidos y de bajo riesgo*" o, alternativamente, permite a los PSP garantizar la salvaguarda de los fondos con una póliza de seguros o garantía bancaria [\[1726\]](#) .

Asimismo, señalan Levi, Shakespear, Liefeldt y Schreiber que Brasil también reguló a los PSP, pero por vía legislativa hace ya 7 años, mediante la Ley N° 12.865/2013 de "*Arranjos e Instituições de Pagamento*". Dicha ley, al igual que en el caso europeo, también otorga al regulador brasileño la función de supervisar a los PSP y de someterlos a un proceso de licenciamiento previo, dejando no obstante fuera del alcance a aquellos participantes que no presenten un volumen significativo de operaciones.

El regulador brasileño también establece requerimientos de capitales mínimos, requisitos de liquidez y reglas en cuanto a la gestión de los riesgos. Respecto de los recursos mantenidos en cuentas de pago, se restringe expresamente a los PSP la posibilidad de que efectúen operaciones que son reservadas a las entidades financieras, obligándolas a mantener los saldos en el Banco Central de Brasil o bien invirtiéndolos en títulos públicos federales. En este sentido, también aquí se determina por ley la separabilidad del patrimonio del PSP respecto de los fondos mantenidos por cuenta de los usuarios, protegiendo a estos últimos de los reclamos de terceros acreedores del PSP en casos de insolvencia o ante otros supuestos [\[1727\]](#) .

Afirman los autores citados que el caso brasileño es similar al europeo en el sentido de que no se limita a regular específicamente algún aspecto particular de la operatoria de los PSP, sino que cambia en forma general la regulación del sistema de pagos del país (yendo hoy hacia un esquema tipo *open banking*), estableciendo, asimismo, reglas de interoperabilidad, vinculación con el sector bancario y apertura de la competencia, garantizando la protección del usuario financiero [\[1728\]](#) .

4.5.13.8. Situación de los Exchanges de criptoactivos: ¿son PSPs?

Branciforte se pregunta si las Comunicaciones “A” 6859 y 6885 son aplicables a los *Exchanges* de criptoactivos como Ripio y Satoshi Tango en otros [\[1729\]](#), ya que las normas citadas establecen que los PSP son aquellos que ofrecen cuentas de pago que permitan recibir o realizar pagos, *pero no aclara en qué billete o activo* [\[1730\]](#).

Así, se ha señalado que debe distinguirse entre (i) los *Exchanges* de criptomonedas que se limitan a ser una plataforma donde las partes se ponen de acuerdo en el intercambio de activos digitales *peer-to-peer*; y (ii) aquellas que generan toda una plataforma y ellas mismas establecen el valor del activo digital, permitiendo crear *Wallets* en las cuales se puede “cargar” tanto moneda de curso legal como moneda extranjera o criptomonedas, y luego con esos valores se puede realizar pagos de, por ejemplo, servicios públicos [\[1731\]](#). En este último caso, tales entidades podrían encuadrar también en el concepto de PSP, ya que justamente permiten recibir pagos (en cualquier tipo de moneda o activo digital) y también realizar pagos con los fondos allí dispuestos, pero existe otro problema ¿Cómo obligar a dichos *Exchanges* que manejan activos digitales con un valor variable segundo a segundo, a tener cuentas a la vista en Pesos con los fondos de los clientes? Por ello se ha sostenido con mucha razón que si bien los *Exchanges* de criptomonedas podrían encuadrar como PSP, las Comunicaciones bajo análisis no fueron realizadas pensando en ellas [\[1732\]](#).

En tal sentido, se afirma que sería recomendable que el BCRA emita una nueva comunicación para encuadrar específicamente a los *Exchanges*, ya que muchas veces pasa que el cliente de la entidad recibe una determinada cantidad de fondos en criptomonedas, dichos fondos son verificados y aceptados por la *blockchain* principal del activo digital y los fondos son cargados en la dirección pública del cliente, pero tardan días y hasta semanas en ser cargados en las *Wallets* de los *Exchanges*, cuando la transacción se hizo en cuestión de minutos, esto hace que si bien el cliente sabe que tiene los fondos, no puede disponer de ellos, y esto hasta podría generar una pérdida

de valor por la volatilidad de los activos en juego [\[1733\]](#).

4.6. *Dinámicas (contractuales) de Creación, Estandarización, Comercialización y Adquisición de Tokens*

Cuando las empresas deciden fondear su operatoria –STOs– o comercializar sus bienes y servicios –ICOs– pensando en clave de tokenización, lo más frecuente será que tengan, internamente, un equipo de técnicos expertos en programación en relación de dependencia, y con conocimiento de lenguajes de programación muy específicos para escribir las líneas de código de los contratos inteligentes que utilicen. Por tanto, usualmente no sub-contratarán a un tercero la programación del contrato inteligente que transaccionará los tokens a crear, pero probablemente sí contraten servicios de auditoría a expertos en detectar vulnerabilidades en contratos inteligentes antes de desplegarlos en *blockchain*.

A su vez, las empresas que deciden crear y ofrecer masivamente tokens digitales, recurrirán normalmente a un *Exchange* que permita ofrecer, vender y *tradear* estos tokens, de modo de (i) ganar reputación si consiguen que un *Exchange* respetable les permita “listar” su token en su plataforma, “tercerizando” en el *Exchange* el cumplimiento de normas de KYC-AML respecto de los adquirentes, y, además, (ii) tener acceso a la base de clientes del *Exchange*.

Así, el proceso de aceptación de un token por parte de un *Exchange* sería –*mutatis mutandis*– similar al proceso descrito *supra* en § 3.5.1.3.3.1.3 al describir la Guía de Selección de Proyectos de una Plataforma de Financiamiento Colectivo, y puede incluir un due diligence más o menos profundo, incluyendo la auditoría del *Smart Contract* ofrecido. Por ejemplo, *Binance*, el *Exchange* más grande del mundo revisa periódicamente los siguientes aspectos de todos los tokens que ofrece, para decidir si los mantiene o los remueve de su plataforma:

- (i) Commitment of team to project
- (ii) Quality and level of development activity

- (iii) **Network / Smart Contract stability**
- (iv) Level of public communication and activity
- (v) **Responsiveness to our periodic due diligence**
- (vi) **Evidence of unethical / fraudulent conduct**
- (vii) Contribution to a healthy and sustainable crypto ecosystem [\[1734\]](#)

Evidentemente, el proceso de negociación entre un emisor/creador de un token y un *Exchange* puede ser largo y tedioso, ya que el *Exchange* compromete su seriedad (cuando no su responsabilidad) si admite listar tokens que resultan ser un fiasco o un fraude. ¿Cuánto cuesta el permiso de un *Exchange* para ser listado? En Agosto de 2018, una pelea muy mediática tuvo justamente por causa el alto precio que un *Exchange* cobraba por listar tokens de un emisor: aparentemente 400 bitcoins [\[1735\]](#). Han existido casos de listado de tokens y de *deslistado* de tokens “sospechosos” [\[1736\]](#) y también *Exchanges* que “donan todas las comisiones que cobran” para caridad [\[1737\]](#).

Ahora bien, se ha sostenido que el *boom* de ICOs de 2017 –que fue luego seguido por el *CryptoWinter* [\[1738\]](#)– se debió principalmente a startups de todo el mundo ofreciendo utility tokens del tipo ERC20 en Ethereum [\[1739\]](#). ERC significa *Ethereum Request for Comments* y definen una serie de reglas estándar [\[1740\]](#).

Esta especie de token es realmente muy fácil de crear, tiene tres reglas optativas y seis reglas obligatorias que deben cumplir todos los *Smart Contracts* que los crean. Las seis reglas obligatorias son: cantidad total de tokens que se crearán [\[1741\]](#), saldos acreditados en cuentas [\[1742\]](#), transferencias [\[1743\]](#), formulario de transferencia y aprobación [\[1744\]](#) y consulta de saldo en cuenta [\[1745\]](#). Las tres reglas optativas son: nombre,

símbolo y decimales (hasta 18 decimales ^[1746]). Todos los tokens creados con ERC20 pueden ser transferidos, intercambiados con otros tokens ERC20, o gastados, pero no pueden programarse limitaciones a la transferencia de los tokens.

La gran utilidad de este tipo de tokens ERC20 es la gran estandarización de sus términos, ya que todos los contratos inteligentes que crean estos tokens usan el mismo tipo de reglas y el mismo lenguaje de programación. Otros tipos de tokens son el ERC1400 ^[1747] pensado específicamente para security tokens, y que permite programar reglas que limitan la transferencia del token de acuerdo a lo que estipulan las normas de oferta pública de títulos valores, o el ERC721, para tokens no fungibles, y utilizado para los *cryptocollectibles* ^[1748].

Pero antes de llegar al contrato que se celebre con un *Exchange*, es probable –aunque no siempre ocurre– que la empresa haya celebrado contratos de *pre-financing* tipo *SAFTs* con ciertos inversores, desarrollados *supra* en § 3.3.1.2.1, o directamente haya pre-venido tokens a un precio preferencial para fondear el desarrollo, *pre-sales*, hasta tanto éste es aceptado por un *Exchange* y vendido masivamente.

Naturalmente, como se ha visto, si el token creado, según el White Paper, puede ser encuadrado como un valor negociable, *security* o algún otro tipo de producto de inversión con oferta pública regulada, cualquiera sea la jurisdicción, la empresa deberá registrar esos tokens como STOs, o bien conseguir un tratamiento de excepción como un ICOs.

La mayoría de estas dinámicas contractuales se podrán celebrar mediante contratos electrónicos a distancia, o en papel celebrados entre presentes, y serán negociados y paritarios, o celebrados por adhesión. Las dinámicas contractuales en materia de creación y comercialización de tokens, normalmente serán relaciones comerciales B2B, entre empresarios. Sólo los contratos de adquisición de tokens podrán ser, según el caso, contratos encuadrables como contratos con consumidores, en tanto se den las condiciones exigidas por el Estatuto del Consumidor.

Desde el punto de vista del adquirente de un token, evidentemente debe

tener ciertos conocimientos en tecnología y también en la materia de negocio sobre la cual la empresa que emite un token desea operar, y para la cual busca clientes –ICOs– o inversores –STOs–. Recordar que los derechos que el token confiera están escritos en el código del *Smart Contract* que utilicen, y por ende, todos los riesgos de codificación deficiente deben ser debidamente ponderados y comprendidos [\[1749\]](#). Como la compra de tokens se realiza normalmente mediante contratos electrónicos, será de aplicación lo previsto en el Art. 1107, CCCN y el vendedor del token deberá informar sobre los riesgos específicos derivados de su adquisición por medio electrónico, y quién asume dichos riesgos.

Finalmente, no debe olvidarse que el riesgo de venta de tokens fraudulentos es muy alto. Con gran precisión, señalaba la doctrinaria rusa Alina Myalo [\[1750\]](#) que los fraudes en materia de ICOs alcanzaron al 81% de todas los ICOs creados entre 2017 y 2018; otro 11% restante no tuvo éxito por cuestiones de negocio, y sólo un 8% llegó a completar el proyecto fundado de manera exitosa, a lo que se suma que el 10% de los fondos recaudados vía ICOs fueron robados por cibercriminales. En efecto, y como ejemplo, véanse los casos de *OneCoin* y *GNO* [\[1751\]](#), dos tokens que básicamente ofrecían la misma propuesta de inversión, y que son una buena muestra de lo difícil que puede ser para un inversor de tokens separar la paja del trigo. El token *GNO* de la empresa Gnosis [\[1752\]](#) recaudó en 12 minutos 12 millones de Dólares al poner en venta el 5% del proyecto, mientras que *OneCoin* defraudó a inversores en todo el mundo por valor de 350 millones de Dólares [\[1753\]](#). Con mucha razón se ha sostenido que:

“There are few barriers to participation aside from knowing how to conduct a Bitcoin transaction, and **the space mostly lacks the robust independent analysis performed by underwriters in the IPO market**, which can help tamp down overoptimism. **The risk isn’t just to individual investors**; many argue that the mania of the late-1990s internet bubble ultimately slowed the entire sector down by making investors

skittish for years afterwards. Imagine how much worse things might have been if the whole thing had been entirely unregulated. **Careful regulation, then, could protect blockchain projects from a hugely damaging bust.** And the model is genuinely utopian enough to deserve nurturing. Cryptographic tokens effectively make all of a platform's users part-owners. Anyone selling goods for Bitcoin, for example, has had a chance to benefit from its huge price boost over the past year, while Facebook and Google users have not shared in those companies' growth. [\[1754\]](#),” (el resaltado es mío).

Werbach ha sostenido que estos riesgos de las ICOs fraudulentas son muy similares a los que ya se vivieron en la década del 1930, y que justificaron en EE.UU el dictado de leyes específicas y la creación de reguladores altamente especializados –SEC–, y que apuntan precisamente a evitar fraudes, obligan a registrar los títulos valores salvo excepciones, y exigen difundir información materialmente relevante sobre cada propuesta de inversión lanzada al mercado [\[1755\]](#).

En este sentido, la difusión de información es la idea fuerza que sustenta todas las leyes de títulos valores con oferta pública del mundo [\[1756\]](#), que buscan *quebrar* la asimetría de la información, para proteger al inversor, siempre que lo ofrecido sea, en su sustancia y esencia, un título valor [\[1757\]](#).

Una investigación del WALL STREET JOURNAL durante 2018 [\[1758\]](#) donde se analizaron en profundidad 1450 criptomonedas ofrecidas, detectó casos de fraude, robo de identidad y promesas de retornos irrealizables, además de, obviamente, publicidad engañosa. De las 1450 criptomonedas analizadas, en 271 se detectaron incluso supuestos equipos de personas a cargo de proyectos que en realidad no existían, eran identidades falsas, o más técnicamente, robo de identidad de otras personas, que hacían promesas incumplibles de retornos ficticios. Se iniciaron en el mismo año muchas demandas por inversores engañados, por 271 millones de Dólares.

De los 1450 White Papers analizados, en 111 se encontraron las mismas secciones, el clásico *copy & paste*, 48 proyectos ni siquiera tenían un web site activo, e incluso 25 garantizaban una rentabilidad al inversor [\[1759\]](#), algo que está expresamente prohibido por la SEC.

4.6.1. *Protegiendo al adquirente de tokens digitales a través del Legal Design*

Es cierto que el adquirente medio de un token normalmente tendrá ciertos conocimientos en tecnología –sin llegar a ser un programador, necesariamente–, además de comprender el *problem-solution-fit* que ofrece el emisor del token como propuesta de valor.

Ahora bien, se ha señalado que éste ámbito, el de la venta de tokens a nivel global, puede ser un campo propicio para implementar técnicas de visualización contractual tendientes a facilitar la comprensión de las relaciones contractuales, legales y programadas, subyacentes [\[1760\]](#). Esto demandará un *rol nuevo* para los Abogados, en el que se convierten en *ingenieros de transacciones* y *Project Managers* de equipos multidisciplinarios.

En este sentido, se afirma, en opinión que se comparte plenamente:

“In the context of the digital revolution, **lawyers therefore need to focus on re-discovering their function as effective transaction engineers that can assist parties in facilitating interactions and reducing costs.** In a modern business environment, there are many costs that need to be cut: agency costs, transaction costs, monitoring costs, regulatory costs, and compliance costs. As such, the scope for lawyers to “add value” is enormous (...) **lawyers of the future will need to be able to assume the role of “project managers.”** Lawyers will need to become key participants in multidisciplinary teams that are going to design the new solutions of the future. A capacity to operate in a multidisciplinary environment will be vital, as the ability to communicate with a more diverse set of “partners” is

increasingly required. The lawyer of the future **will need to understand the opportunities and challenges and help firms to re-invent their governance structures to be more open and inclusive.** In this new world of platforms, such “matchmaking” and project-based temporary partnerships, will mean that **lawyers and other legal advisors will need to be aware of the way network technology, and other code-based technologies operate.** After all, many of the “solutions” that the lawyer of the future will be expected to help design will be technology based. **The transactions that lawyers will be facilitating will be dependent on computer code.** It is in this context that to facilitate lawyers in performing this function, **legal education will need to undergo some important changes** in order to prepare prospective legal professionals to perform this function (...) in the context of the digital transformation, **an understanding of code is going to be crucial for the lawyer of the future to perform this transaction engineer function effectively.** More and more businesses and industries will revolve around code-based products or services, so facilitating transactions—i.e., being an active transaction engineer—will inevitably involve coding to some degree. Such coding will require **multidisciplinary teams working in collaboration and the capacity of lawyers to actively participate in such teams will be crucial to their success as legal professionals.** The development of Blockchain technologies and Smart Contracts are particularly relevant in this regard.”^[1761] (el resaltado es mío).

Se ha sostenido que en materia contractual, los Abogados históricamente ponen el foco en el contenido y la precisión de los términos empleados, sin poner mucha atención en el *usuario* de dicho contenido^[1762]. La novel disciplina del *Legal Design* cambia el enfoque, y pone el foco en el usuario y su experiencia. Consiste en un enfoque multi-disciplinario, que aplica el diseño *centrado en la persona*, para prevenir o resolver problemas legales^[1763]. El

Legal Design analiza la forma en que la información es presentada, cómo se diagraman los procesos intra-contractuales, y cuáles son los criterios y políticas de un contrato dado. El objetivo es mejorar la comunicación contractual, de modo que sea más fácilmente comprensible por sus usuarios.

Evidentemente, este cambio de enfoque no sólo se predica de los contratos convencionales, sino también de sus hermanos más modernos y aún más complejos, los *Smart Contracts* ^[1764]. Así, se ha sostenido que:

“Contract Design **applies design thinking in the context of contracts**, aiming to make them more useful and usable: the focus is on supporting collaboration, driving desirable outcomes, creating opportunities, and preventing problems before they arise. Contract designers do more than drafting: they **look for a balance between functionality and precision, and between precision and ease of use**. This requires contracts and processes that make sense for the people who work with those contracts, whether those contracts are smart or “dumb. **Design thinking stresses the importance of visual communication**. Visualizing helps humans to think, communicate, make assumptions visible, and secure understanding across disciplines. The goal is not to create images—**the goal is to create understanding**. In the context of platforms and Smart Contracts, visualization can help create functional, useful, and usable processes, systems, and outcomes. **It can help lawyers, technologists, and business people see the big picture and communicate and share solutions.**”^[1765] (el resaltado es mío).

En este sentido, la visualización –i.e, utilizar gráficos, tablas, diagramas e imágenes para complementar el clausulado contractual– ayuda al usuario a entender información compleja, entender el significado de lo expuesto, y aclarar el alcance de los derechos y obligaciones del contrato. Repárese que las partes de un contrato, excepto que se trate de un contrato formal, pueden

siempre libremente elegir la forma de expresar su intención, normalmente a través de palabras, pero también puede ser a través de líneas de programación, gráficos e imágenes, tal como ya ocurre con algunas licencias de Creative Commons [\[1766\]](#).

Los Abogados agregarán valor a sus clientes –y por ende, podrán capturarlo en forma de mejores honorarios– si puedan producir un producto literario – i.e., un contrato– que sea fácilmente entendible, complementando el lenguaje natural legal super sofisticado y propio de nuestro *expertise*, con diagramas que grafiquen, por ejemplo, el ciclo de transacciones, gráficos e íconos. Al respecto, es muy interesante el trabajo sobre diagramación contractual de Kevin Conboy [\[1767\]](#).

Como Abogados, nos ha llegado la hora de importar buenas prácticas de otras profesiones. Los arquitectos de software, los programadores y los diseñadores están acostumbrados a utilizar *patrones de diseño*, como una forma de utilizar soluciones ya probadas para la resolución de problemas [\[1768\]](#). Estos patrones de diseño [\[1769\]](#) serán cada vez más frecuentes, a medida que la digitalización de la Economía penetre en todos los sectores, proceso que sin dudas se ha acelerado por la pandemia del COVID-19.

En materia de *Smart Contracts*, con un ojo puesto en el derecho a la información del consumidor y usuario, que tiene derecho a recibir *información cierta, detallada y proporcionada con claridad necesaria que permita su comprensión* [\[1770\]](#), recurrir a la visualización contractual puede significar la noche o el día en la masificación de su uso [\[1771\]](#), dado que muy pocos usuarios tendrán los conocimientos de programación para entender, por sí mismos, qué están por contratar, o cuáles son los riesgos inherentes, quién los asume, o las responsabilidades emergentes.

En este sentido, se ha sostenido que:

“The challenges of those people preparing Terms of Service

or other consumer-facing terms are very similar to the challenges faced by the people preparing privacy policies: the audience consists of individuals who are most often reluctant to read and seldom have a chance to negotiate. The challenges of those preparing Data Processing Agreements between processors and controllers, again, are to some extent similar, but in other respects, they resemble those encountered by commercial contract drafters (...) The key challenges in **commercial contracting relate to the number of people involved in preparing, making, implementing and monitoring the contracts and the multitude of the parties obligations** (...) To be useful, **patterns should be written with their intended audience in mind**. Contracts and related design patterns, for example, are not about legal information alone, and they should take into account the different professions that may be involved in preparing the contract documents. We could call them drafters, crafters or designers, but call them writers here. **Readers' (or non-readers') problems are at the same time also writers' problems**. When responding to the problems of the former, the patterns at the same time respond to the problems of the latter. **Design-minded writers seek to make life easier for the users of their work products**. In commercial contracting, the writer may be a lawyer or a contracts or commercial professional, the contract users are often business managers and negotiators who do not have a law degree: approvers, operational or delivery team members, accountants, and so on - busy and business-savvy people, only occasionally a regulator or a judge. [\[1772\]](#)” (el resaltado es mío).

Un patrón de diseño contractual estándar debiera tener estos seis elementos, idealmente: (1) *resumen*: se define el patrón elegido; (2) *problema*: se definen y explican los problemas que el patrón de diseño busca resolver en el contrato; (3) *solución*: explica cómo el patrón de diseño elegido puede resolver el problema identificado; (4) *objetivos*: enumera los objetivos que el patrón de diseño busca alcanzar; (5) *limitaciones y consecuencias*: se definen

las limitaciones y condiciones que han debido respetarse para implementar el patrón de diseño y cuáles son las consecuencias y resultados esperados por aplicar el patrón en cuestión; y (6) *ejemplos*: en los que el patrón de diseño es utilizado dentro del contrato [\[1773\]](#).

Se han puntualizado ejemplos de patrones de diseño contractual, tales como usar lenguaje plano y evitar los tecnicismos legales, usar letras con tamaño y formato legibles, utilizar ejemplos para ilustrar el funcionamiento de determinadas cláusulas sensibles, utilizar títulos y secciones de manera adecuada, utilizar un índice al inicio, con hipervínculos a las secciones del contrato, colocar avisos y notificaciones del tipo pop-up en cláusulas sensibles, utilizar tablas y gráficos, estimar e informar el tiempo de lectura requerido para el contrato, establecer un mecanismo que informe el grado de progreso en la lectura del contrato, visualizar la relación contractual utilizando mapas de viajes (origen, viaje y destino) [\[1774\]](#), utilizar íconos para identificar determinado tipo de cláusulas, o derechos u obligaciones críticas, utilizar video tutoriales, preparar una lista de preguntas y respuestas frecuentes, ajustada al contrato, y, si existe suficiente presupuesto, programar un chatbot para responder a las preguntas legales del usuario [\[1775\]](#).

Sin dudas, existe mucha utilidad –y gararán creciente espacio y mejores roles los Abogados que lo hagan– en comenzar, de a poco, a pensar, escribir y diagramar los contratos y sus flujos de derechos y obligaciones con una *mirada empática*, centrada y muy concentrada en la experiencia del usuario, máxime si se trata de contratos electrónicos inteligentes, escritos en doble idioma, el natural legal, y el de programación de la *blockchain* de que se trate. A la inversa, será también a todas luces beneficioso tanto para los proveedores de *Smart Contracts* como para las empresas que decidan utilizarlos para comercializar sus bienes y servicios, facilitar la experiencia del usuario, recurriendo a la visualización contractual, y otras herramientas que ayudan a volver simple lo complejo, a volver más claro lo oscuro. En efecto, si bien la computación puede y debe generar confianza, i.e. *trust-by-computation*, lo cierto es que sin transparencia en cómo esa confianza opera y se genera, los círculos de confianza así creados serán demasiado pequeños, y estarán reservados a aquéllos que han tenido la suerte de poder formarse en ciencias

de la computación.

4.7. Responsabilidad de las plataformas de blockchain

Luigi Buonanno, en un interesantísimo y premiado trabajo titulado *Civil liability in the Era of New Technology: the influence of blockchain* [\[1776\]](#), sostiene que el auge de la *blockchain* producirá el surgimiento de nuevos principios en el Derecho Privado, toda vez que la naturaleza descentralizada de la cadena de bloques dificulta identificar a una persona u organización civilmente responsable en casos de malfuncionamiento o de actividades ilegales realizadas a través de *blockchain*. Buonanno va incluso más allá, y propone aplicar un enfoque de responsabilidad objetiva basada en el riesgo de esta tecnología, dejándose de lado los criterios de responsabilidad subjetiva basados en la culpa del agente, y postula el establecimiento legal de una obligación expresa de contratar seguros en cabeza de todos los operadores de una *blockchain*, con el ojo puesto en la indemnización de daños causados a consumidores y usuarios finales.

4.7.1. El Derecho Privado ante la blockchain

El derecho europeo continental –del cual dimanaron y se han extraído nuestras reglas de derecho privado en general e incluso de ciertos estatutos específicos muy relevantes, como el caso de nuestro régimen de defensa de la competencia–, comienza a tomar conciencia del fuerte impacto que las nuevas tecnologías, especialmente la Inteligencia Artificial, producirá en el sistema de responsabilidad civil.

En el caso de *blockchain*, téngase en cuenta que el caso *TheDAO* ocurrió en Alemania, con lo cual esta nueva realidad de organizaciones virtuales se apersonó en el corazón de Europa y dentro de su economía más pujante y dinámica. El *hard fork* de Ethereum, y el *hard fork* de Bitcoin de 2013, a su vez, dejaron en claro que la inmutabilidad de la *blockchain* es relativa y que el registro puede ser adulterado por una mayoría de nodos que lo consientan [\[1777\]](#).

Buonanno hace las preguntas correctas. ¿La responsabilidad de un fundador/operador de una *blockchain* es similar a la de un proveedor de servicio de Internet –*ISPs*–? Evidentemente, no. El control que un ISP puede ejercer sobre contenidos que circulan y se publican en Internet no tiene nada que ver con la posibilidad de control que existe en una red descentralizada; y salvo en el caso de *blockchains* privadas o consorciadas, en *blockchains* públicas no existe una entidad u organización que pueda remover un *criminal Smart Contract*. El autor citado sostiene que la *blockchain* puede ser considerada un servicio ofrecido a los usuarios, una herramienta *peer-to-peer*, que permite realizar ciertas transacciones. Siendo calificada como un *servicio*, afirma Buonanno que no le son aplicables las normas existentes sobre productos defectuosos [\[1778\]](#), y que será necesaria una nueva legislación que aborde los servicios *algorítmicos* en general, y la *blockchain* en particular, ya que no existe duda, según el autor, que la cadena de bloques se convertirá en el sistema de referencia para transacciones humanas [\[1779\]](#).

4.7.2. Responsabilidad objetiva en entornos de blockchain

Buonanno sostiene que cualquier legislación que se dicte, debiera consagrar el principio de responsabilidad objetiva en cabeza del operador de una *blockchain*, en su calidad de creador del riesgo, y aún a pesar de su inhabilidad técnica de poder controlar el *uso* que se la da a la *blockchain* de que se trate [\[1780\]](#). Se afirma:

“This is the fundamental rationale of strict liability. If we value the concept that, in some cases, the liable person could be **‘the one who has created a risk which materialises in some manner of damage’**, it consequently seems logical to assume the contractual liability of the founder-operators of blockchain platforms, **individuals who will have promoted the platform by advertising it as highly secure but whose malfunction resulted in the materialisation of damage** (...) The more

blockchain spreads, the more strict liability will be strengthened. The process of secularisation of civil responsibility would thus reach its definitive fulfillment: **a transition from an ethical paradigm (centered on fault) to a legal criterion that can be summarised in the formula of Benedetto Croce according to which ‘one is not responsible; one is instead made responsible’**, thus conforming to his idea of the amoral character of the law and the perfect coincidence of the legal activity with the economic one.”^[1781] (el resaltado es mío).

4.7.3. *Las cláusulas de liberación de responsabilidad*

Puntualiza con razón Buonanno que cuando un usuario decide descargar un programa que le permite operar en *blockchain*, se encuentra con una cláusula de exoneración de responsabilidad civil, advirtiéndole al usuario que él asume los riesgos por el uso de la plataforma^[1782]. Más allá de la invalidez de esta cláusula frente a un usuario o consumidor con destino final, señala el autor citado que es de toda lógica que los riesgos no sean trasladados al usuario, sino soportados por el creador de la plataforma, ya que él es el obligado a garantizar la máxima seguridad del servicio tecnológico que provee, y debe tomar a su cargo la indemnización de daños y perjuicios que el malfuncionamiento de la plataforma pueda ocasionar^[1783].

Afirma Buonanno que los casos preexistentes de *hard forks* de Ethereum y Bitcoin permiten sostener que los operadores, i.e. los nodos, pueden prevenir los daños e incluso compensarlos, volviendo atrás operaciones perjudiciales^[1784]. El autor citado argumenta en estos términos:

“Although, in some cases, end users have been involved in the remedial choice of opting for a hard or soft fork in blockchain platforms, this cannot constitute a valid reason for exempting the relevant operator from liability where there are (...) crypto-

economic losses to the detriment of the end users. Recourse to the concept of remedy, which has the function of repairing the damage suffered, presupposes the existence of liability. There is still someone who, by putting the algorithmic service into circulation, decides to assume the risk that in spite of adopted precautions (in terms of safety and immutability), the activity will materialise in damage. Paradoxically, a total absence of responsibility would also weaken the incentive to take the abovementioned precautions, imposing a net cost on society, which would ultimately become a burden for the victims of the damage.”[\[1785\]](#)

4.7.4. Seguro obligatorio de responsabilidad civil

Coherente con su pensamiento, Buonanno considera que la responsabilidad objetiva que pesa sobre los operadores de una *blockchain* debe, obligadamente, ser asegurada, del mismo modo que se ha sugerido hacerlo en materia de daños causados por uso de robótica [\[1786\]](#).

Se afirma:

“In fact, where the value of cryptocurrency stolen by a hacker on a decentralised platform would be greater than the financial resources of the relevant operator, the risk borne by the end users of not being fully compensated would be enormous and unjustified. It is true that the amount of the insurance premium payable by the blockchain operator would be sizeable in monetary terms, but it would never be equal to the immensely higher value of each theft that has occurred over the last few years on decentralised platforms.”[\[1787\]](#)

4.7.5. El enfoque norteamericano

Del otro lado del Atlántico, la cuestión de la responsabilidad civil en entornos *blockchain* también genera mucho debate. En este sentido, Robert Schwinger [\[1788\]](#) sostiene que se pueden teóricamente detectar responsabilidades eventuales en cabeza de los desarrolladores de una *blockchain* en tanto plataforma, en cabeza de los mineros que la mantienen y actualizan, en cabeza de los usuarios finales de la misma y, finalmente, también en cabeza de los desarrolladores de *Smart Contracts* que corren en la *blockchain*. En la visión de la *Commodity Futures Trading Commission*, la responsabilidad por daños causados por un *Smart Contract* debe imponerse, principalmente, a los desarrolladores del contrato, y no a las demás partes involucradas [\[1789\]](#).

Ahora bien, con relación a la responsabilidad civil de las plataformas de *trading*, Schwinger puntualiza que existe un caso actualmente en litigio mientras estas líneas se escriben, *Berk v. Coinbase* [\[1790\]](#), que involucró el *hard fork* de Bitcoin que generó la criptomoneda conocida como *Bitcoin Cash* (BHC). En el caso se intentó una acción de clase basada en el Estatuto del Consumidor, alegando que el *Exchange* actuó fraudulentamente al momento de difundir a sus clientes que BHC salía a la venta, autorizando el *trading* antes de tiempo y suspendiéndolo luego de 3 minutos, por lo que se alegó que había habido un uso ilegal de información privilegiada, *insider trading* [\[1791\]](#). El Juez del caso descartó la existencia de *insider trading*, pero el juicio sigue su curso.

Schwinger también analiza el caso de la legislación del Estado de Vermont, que creó la *Blockchain-based Limited Liability Company* [\[1792\]](#), y que permite limitar la responsabilidad del operador, de los nodos, y de los usuarios de una *blockchain* que asuma esta novedosa e interesante forma jurídica. Como se dijo antes, el Derecho tiene una larga tradición en reconocer personalidad jurídica a ciertas *ficciones*, y de limitar la responsabilidad de los miembros de tales ficciones [\[1793\]](#).

También es muy interesante el enfoque de Zetsche, Buckley y

Arner [\[1794\]](#), también norteamericanos, que analizan la responsabilidad en entornos *blockchain* según sea contractual, extracontractual, societaria, o derivada de una legislación específica, como la antitrust.

En materia contractual, afirman los autores citados que las partes del contrato que genere una responsabilidad emergente serán las que controlen, gestionen o de cualquier otro modo sean dueños de los agentes electrónicos no humanos. Esta responsabilidad puede encontrarse entre el broker de criptoactivos y sus clientes, y también entre los desarrolladores de una *blockchain* privada y los nodos validadores, y los usuarios de la *blockchain* de que se trate, que descargan el software respectivo.

Sostienen los autores citados que también en casos de *blockchains* abiertas [\[1795\]](#), es posible sostener que existe un contrato que vincula a los desarrolladores de la *blockchain*, los nodos y sus usuarios. Ahora bien, la responsabilidad por un incumplimiento contractual se regirá *también* por los términos del contrato que vincula a las partes. En este sentido, es frecuente encontrar cláusulas de liberación de responsabilidad muy amplias en materia de *open software*, i.e., *open blockchains*, aunque existen muy pocos casos judicializados que hayan analizado si tales cláusulas son o no válidas cuando se oponen a un usuario final de software [\[1796\]](#).

Enseñan Zetzsche, Buckley y Arner que para el derecho norteamericano incluso se podrá establecer una responsabilidad solidaria entre los desarrolladores de la *blockchain* y los nodos, respecto a terceros [\[1797\]](#).

Por otra parte, afirman los autores citados que será procedente la responsabilidad extracontractual en todos los casos donde no se pueda invocar la preexistencia de un contrato [\[1798\]](#), y ante supuestos tales como hackeo, *hard forks* que afecten temporal o definitivamente a los dueños de determinados criptoactivos, esquemas defraudatorios, modificaciones al código de una *blockchain* con dolo o culpa, declaraciones incorrectas o publicidad engañosa, y en general todo tipo de falla de seguridad. Pero ¿a quién demandar? Si se trate de *blockchains* privadas, el caso es (un poco más) claro, ya que será más fácil identificar al desarrollador del software y a los

nodos [\[1799\]](#) .

En tercer término, Zetsche, Buckley y Arner analizan la responsabilidad societaria –mediante la creación de *general partnerships*, equivalentes *mutatis mutandis* a nuestras sociedades de personas–, y también, subsidiariamente, la derivada de un *joint venture* [\[1800\]](#) , aclarando que cada legislación define cuándo existe una sociedad y cuándo no.

Para el sistema norteamericano, si se determinara que existe una sociedad de personas, la responsabilidad de sus socios será solidaria [\[1801\]](#) , existiendo ciertos criterios de common law que pueden incrementar la responsabilidad según se trate de *blockchains* públicas o privadas [\[1802\]](#) .

En cuarto y último lugar, Zetsche, Buckley y Arner analizan la responsabilidad emergente de legislaciones especiales, especialmente la legislación antitrust [\[1803\]](#) , que, en caso de infracción constatada, permite responsabilizar a la sociedad subsidiaria y también a su sociedad controlante [\[1804\]](#) .

Coincidiendo con la postura de Buonanno, Zetsche, Buckley y Arner también se pronuncian a favor de cubrir la responsabilidad civil eventual mediante seguros [\[1805\]](#) . Afirman los autores citados:

“While DLT systems may be very secure from a technological perspective (at least those which are properly designed and built), from a legal perspective, **they may well spread risk that was formerly concentrated in very few parties (or perhaps one party) across all system participants (nodes)**. With the realization that the **failure of a distributed ledger system represents a risk**, financial institutions will have to adjust their business strategies to accommodate the contingent liability involved in DLT. From the standpoint of immutability, once an error is embedded in the blockchain, this may be highly

problematic, legally, in that law often requires the ability to rectify errors as a matter of law in a way foreign to DLT. Instead of rectification, **plaintiffs may turn to compensation.** Likewise, transparency requires careful consideration in design to avoid liability for inadequate data protection. (...) In particular, **liability will not be eliminated but may instead be spread across the system,** and financial intermediaries involved in a distributed ledger should arguably hold capital or acquire insurance for contingent liabilities stemming from DLT participation. Likewise, operators may, in time, need to be governed by regulatory requirements similar to those governing other providers of systemically important infrastructure, such as traditional centralized payment and settlement systems. Liability matters, however, and distributed ledgers may, in time, most often be legally structured (particularly in permissioned systems) as a joint venture where all servers are owned and operated—ironically—by one entity, or a small number of specified entities, rather than as a cooperation among multiple entities.”^[1806] (el resaltado es mío).

Finalmente, por ahora, junto con Schwinger se puede provisoriamente concluir que:

“The legal system is just now starting to grapple with deciding what rights and liabilities are appropriate when disputes arise involving parties who interact in transactions conducted via blockchain technology. **Blockchain ventures and their participants are likely to face an uncertain period of theorizing, experimentation, legislation, regulation and litigation before the legal system comes to consensus on what legal rights they enjoy and what liabilities such participants may face in their dealings with one another.**” (el resaltado es mío).

4.7.5.1. ¿*Hard cases make bad law*? el caso *SEC v. Shavers* [\[1807\]](#)

Los norteamericanos tienen algunas frases célebres, al menos en el mundillo legal. *Hard cases make bad law* es una de ellas [\[1808\]](#). En un interesante artículo de fines de 2019, Sepher Shahshahani, profesor de la Facultad de Derecho de la prestigiosa Universidad Jesuita de *Fordham* en Nueva York, plantea y demuestra un punto que tiene indudable conexión con un Capítulo de un Manual que pretende delinear los trazos gruesos de la responsabilidad civil en entornos de *blockchain* [\[1809\]](#).

Saltando las distancias y grandes diferencias evidentes entre un sistema del common law y un sistema del derecho europeo continental, puede sostenerse que hay un vínculo posible entre un Juez del common law que *legisla* para el caso, y un Juez proactivo como es el mentado en el CCCN, con facultades muy fuertes para ejercer su discreción, de acuerdo a los hechos del caso, en materias tan relevantes como:

- i) obligaciones: en cuanto a intereses en obligaciones de dar dinero (art. 771, CCCN), en supuestos de cláusula penal y sanciones conminatorias (arts. 794 y 804, CCCN) y regulación del pago por consignación judicial (arts. 904 a 909, CCCN),
- ii) contratos, al disponer el control judicial de cláusulas abusivas en los contratos de adhesión (art. 989, CCCN) o en contratos de consumo (art. 1122, CCCN), determinar el precio de la compraventa (art. 1134, CCCN), en la locación de obra (arts. 1255, 1261 y 1265, CCCN), el cobro del saldo ejecutivo en cuenta corriente bancaria (art. 1440, CCCN);
- iii) en materia de responsabilidad civil: al regular la acción preventiva del daño (arts. 1711 a 1713, CCCN), al determinar la aplicación de sanción pecuniaria disuasiva en materia de violación de derechos de incidencia colectiva y moderación de la punición irrazonable o excesiva por condenaciones pecuniarias administrativas, penales o civiles (arts. 1714 y 1715,

CCCN), legítima defensa, estado de necesidad y ejercicio regular de un derecho (art. 1718, CCCN), se prescriben los factores de atribución del daño objetivo y subjetivo con elementos para valoración de la conducta y la relación causal (arts. 1721 a 1727, CCCN), *impone la carga de la prueba de los factores de atribución y de las eximentes de responsabilidad civil* (art. 1734, CCCN), *se faculta expresamente al juez para modificar la carga de la prueba* (art. 1735, CCCN), y se determina quién debe probar la relación de causalidad (art. 1736, CCCN), *contempla la atenuación judicial de la responsabilidad por equidad* (art. 1742, CCCN) y en daños causados por acto involuntario (art. 1750, CCCN), edicta sobre el *onus probandi* en materia de daños (art. 1744, CCCN), prescribe facultad judicial en indemnizaciones por fallecimiento (art. 1745, ap. B, CCCN),

iv) respecto a títulos y valores, en forma taxativa precisa las defensas oponibles de fondo que puede oponer el deudor (art. 1821, CCCN), y contempla el ámbito de aplicación y los efectos de las medidas precautorias (art. 1822, CCCN) [\[1810\]](#).

Por tanto, es a todas luces evidente habrá casos fáciles y habrá casos difíciles en entornos de *blockchain*. Los casos que más abajo se anotan, han sido adrede seleccionados para demostrar la claridad del caso y de su resolución. Nadie podría no compartir los temperamentos judiciales tomados en cada uno de ellos. Son casos *fáciles*, y son buenos precedentes.

Ahora bien, en la próxima década veremos aparecer casos no tan fáciles, y cada vez más difíciles, en entornos de *blockchain*. El caso *TheDAO* ya es un buen ejemplo de una dificultad creciente, que involucra responsabilidades multi-parte en entornos de doble-red: Internet y, arriba, *blockchain*. ¿Imagina el lector el pleito multi-parte multi-jurisdiccional que se habría desatado si no se hubiera implementado el *hard fork* de Ethereum? ¿Repara el lector que este remedio tecnológico de una simil *tecnorestitutio ex ante facto* no es posible fuera de la cadena de bloques? Repare también en que no necesariamente toda la jurisprudencia generada en las últimas tres décadas para una red

también descentralizada –Internet–, servirán para otra red descentralizada de segundo grado, como es *blockchain*.

Una segunda red que opera por encima de una primera red es, por esencia, más riesgosa que la primera, ya que si falla la primera –Internet–, fallará también la segunda. El usuario debe comprender esa diferencia de niveles y de niveles de riesgos entre dos redes superpuestas, así como percibe los beneficios al utilizarlas. Los riesgos de una y otra son muy distintos, al igual que sus funcionalidades.

Así, los Jueces serán expuestos en la próxima década a casos donde, de momento, poca legislación los contempla de manera explícita. De modo tal que se aplicarán –y mucho– las reglas preexistentes, pero en clave de analogía y equidad. Por lo menos, hasta tanto exista un consenso en el Derecho de cómo regular todos los ámbitos de la interacción de los mundos *off-chain* y *on-chain*.

Es por ello que, *in a flat world*, y hasta tanto exista una legislación especial que aborde el entorno *blockchain*, cualquier fallo de cualquier juez del mundo puede influir y debe influir en la regulación del uso y reparto de riesgos de esta nueva tecnología y del entorno que crea, que como se dije antes, es un entorno de red con contratos coligados. Y debe hacerlo como todo en la vida, con sensatez, pasión y sacrificio, y a la vez, como partícipe e intérprete de la sociedad en la que vive, acotaría Calamandrei.

Pero volvamos a Shahshahani, quien cita a Oliver Wendell Holmes, quien afirmaba que no solo los casos difíciles pueden hacer malas leyes –i.e., sentencias–, sino también los casos *importantes*:

“Great cases, like hard cases, make bad law. For great cases are called great, not by reason of their real importance in shaping the law of the future, but because of some accident of immediate overwhelming interest which appeals to the feelings and distorts the judgment. These immediate interests exercise a kind of hydraulic pressure which **makes what previously was clear seem doubtful, and before which even well settled principles of law will bend.** [\[1811\]](#)” (el resaltado es mío).

Ahora bien, ni por un momento se dude que la posibilidad de creación de valor digital –*tokens*– que ofrece la *blockchain*, y que es algo muy distinto y superior al dinero electrónico que permitió crear Internet –donde la *oferta* de dinero de curso legal no viene dada por la Internet, que sólo lo digitaliza al efecto de darle una mayor tranzabilidad–, los casos que se presentarán en entornos de *blockchain* serán, además de difíciles, casos importantes que pueden, incluso, crear nuevos principios del Derecho que a la fecha aún no hemos descubierto. Pero también habrá cada vez más, como se dijo antes, casos fáciles, como el que se comenta seguidamente.

Trendon Shavers creó un fideicomiso, llamado *Bitcoin Savings and Trust* (BTCST) a través del cual defraudó a inversores apropiándose de 700.000 bitcoins entre 2011 y 2012^[1812]. La SEC demandó alegando violación de las normas federales sobre títulos valores, demostrando que Shavers ofrecía via Internet inversiones a través de BTCSV, con una renta semanal del 7% o del 1% diaria, derivada de la venta de bitcoins a compradores que quisieran actuar “fuera del radar”^[1813] comprando bitcoins pagando en efectivo^[1814].

En el máximo momento de su ardid, Shavers llegó a controlar el 7% de todos los bitcoins en circulación^[1815]. La realidad, que se acreditó en el juicio, era un clásico esquema defraudatorio del tipo Ponzi, pero 100% digital, donde los nuevos inversores pagaban las rentas que correspondían a los precedentes inversores.

BTCSV no había sido inscripto ante la SEC. El ticket mínimo de inversión era inicialmente 50 bitcoins, luego subió a 100 y llegó a engañar a 100 inversores^[1816]. La SEC demostró que:

“BTCST did not sell BTC to individuals who wanted to buy BTC off the radar, quickly or in large quantities; BTCST was not in the business of buying and selling BTC; and BTCST did not generate returns for its investors through such BTC market

arbitrage. Shavers obtained at least 700,467 BTC in principal investments from BTCST investors (...) During the relevant period, Shavers returned at least 507,148 BTC to BTCST investors as withdrawals or purported interest payments (...) Shavers transferred at least 150,649 BTC to his personal account at an online BTC currency exchange which, among other things, he then sold or used to day-trade (converting BTC to U.S. dollars and vice versa) (...) Shavers transferred \$147,102 from his personal account at the online BTC currency exchange to accounts he controlled at an online payment processor and his personal checking account, which he then used for, among other things, his personal expenses, including rent, car-related expenses, utilities, retail purchases, casinos, and meals.” [\[1817\]](#)

En 2014, Shavers fue arrestado y condenado civilmente por un Tribunal de Texas a pagar 40 millones de Dólares en concepto de indemnización, y se impusieron multas de 150.000 Dólares a él y a su fideicomiso. En 2016, fue condenado por un Tribunal penal de New York a un año y medio de prisión efectiva en un juicio abreviado [\[1818\]](#). Evidentemente, este es un caso *fácil*.

4.7.5.2. *El caso Munchee, Inc.*

En Diciembre de 2017, la SEC presentó un pedido judicial de orden de cese contra la empresa californiana Munchee, Inc., que se avino a la demanda [\[1819\]](#). El caso involucró una aplicación para iPhones desarrollada por Munchee, que permite rankear restaurantes. En Octubre de 2017, Munchee creó y ofreció para la venta y vendió un poco más de la mitad de los 500 millones de MUN Tokens creados en Ethereum, y recaudó 15 millones de Dólares que serían aplicados para mejorar su app, reclutar usuarios que escribieran *reviews* de restaurants, o que quisieran vender comidas y hasta podrían contratar publicidad en la app usando los tokens [\[1820\]](#).

Munchee afirmó que sus tokens tendrían negociación secundaria en mercados secundarios y que incrementarían de valor por sus esfuerzos, y

publicó el respectivo White Paper, donde expresamente se hacía referencia al informe de la SEC en el caso *TheDAO*, pero afirmaba expresamente que sus tokens eran *utility* tokens y no un security token [\[1821\]](#).

En su demanda, la SEC remarcó:

“Munchee offered MUN tokens in order to **raise capital to build a profitable enterprise**. Munchee said that it would use the offering proceeds to run its business, including hiring people to develop its product, promoting the Munchee App, and ensuring “the smooth operation of the MUN token ecosystem.” While Munchee told potential purchasers that they would be able to use MUN tokens to buy goods or services in the future after Munchee created an “ecosystem,” **no one was able to buy any good or service with MUN throughout the relevant period**. On the Munchee Website, in the MUN White Paper and elsewhere, Munchee described the “ecosystem” that it would create, stating **that it would pay users in MUN tokens for writing food reviews and would sell both advertising to restaurants and “in-app” purchases to app users in exchange for MUN tokens**. Munchee also said it would work with restaurant owners so diners could buy food with MUN tokens and so that restaurant owners could reward app users – perhaps those who visited the restaurant or reviewed their meal – in MUN tokens. **As a result, MUN tokens would increase in value.**” [\[1822\]](#) (el resaltado es mío).

Munchee, Inc. se avino y devolvió los fondos a los inversores sin reconocer ni rechazar los hechos invocados por la SEC [\[1823\]](#).

4.7.5.3. *El caso SEC v. AriseBank*

En este caso, la SEC demandó a AriseBank y sus fundadores [\[1824\]](#), sosteniendo que los demandados estaban públicamente ofreciendo títulos valores sin previa autorización. Sostuvo la SEC:

“AriseBank purports to be the world's first "decentralized" bank, allegedly offering a variety of consumer-facing banking products and services and supporting more than 700 different virtual currencies. Claiming to be "one of the largest cryptocurrency platforms ever built," AriseBank says it is "focused on bringing cryptocurrency to the average consumer and using it to revolutionize banking. AriseBank began raising money at least as early as November 2017, through a securities offering of AriseCoin—its own digital currency. AriseCoin is being offered in an initial coin offering (“ICO”) through which AriseBank claims it has raised more than 600 million, with a goal of 1 billion. The ICO is an illegal offering of securities because there is no registration statement filed or in effect with the SEC, nor is there an applicable exemption from registration.” [\[1825\]](#)

Los demandos transaron la demanda en Diciembre de 2018 [\[1826\]](#), aceptando pagar 2.7 millones de Dólares en multas.

4.7.5.4. *El caso CFTC v. McDonnell*

En Enero de 2018, la Commodity Futures Trading Commission inició una acción civil en un Juzgado Federal de Nueva York contra Patrick McDonnell y su empresa Coin Drop Markets (CDM) [\[1827\]](#).

La CFTC alegó y probó que CDM ofrecía públicamente servicios de asesoramiento en *trading* de criptomonedas a inversores y ofrecía ganancias garantizadas del 300% semanal [\[1828\]](#), pidiéndoles que depositaran sus

criptoactivos en CDM. Al poco tiempo de captar los fondos, CDM desapareció del mercado. En Agosto de 2018, se dictó sentencia, condenando a los demandados a restituir los criptoactivos y pagar 1.2 millones de Dólares en daños y perjuicios [\[1829\]](#).

En el caso, el Juez sostuvo:

“Until Congress clarifies the matter, the CFTC has concurrent authority, along with other state and federal administrative agencies, and civil and criminal courts, over dealings in virtual currency. An important nationally and internationally traded commodity, virtual currency is tendered for payment for debts, although, unlike United States currency, it is not legal tender that must be accepted (...) Until Congress acts to regulate virtual currency the following alternatives appear to be available: 1. **No regulation** (...) 2. **Partial regulation through criminal law prosecutions** of Ponzi-like schemes by the Department of Justice, or state criminal agencies, or civil substantive suits based on allegations of fraud 3. **Regulation by the Commodity Futures Trading Commission** 4. **Regulation by the Securities and Exchange Commission ("SEC")** as securities. 5. **Regulation by the Treasury Department's Financial Enforcement Network ("FinCEN")**. 6. **Regulation by the Internal Revenue Service ("IRS")** 7. Regulation by private exchanges. 8. **State regulations** 9. A combination of any of the above (...) Legitimization and regulation of virtual currencies has followed from the CFTC's allowance of futures trading on certified exchanges (...) Virtual currencies can be regulated by CFTC as a commodity. Virtual currencies are "goods" exchanged in a market for a uniform quality and value (...) The jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities.” [\[1830\]](#) (el

resaltado es mío).

4.7.5.5. *El caso Skatteverket v. Hedqvist*

En Octubre de 2015, se decidió una cuestión prejudicial por el Tribunal de Justicia de la Unión Europea, elevada por el Tribunal Supremo Contencioso-Administrativo de Suecia [\[1831\]](#). La causa tenía naturaleza tributaria, ya que el organismo fiscal sueco (*Skatteverket*) pretendía determinar en contra de Hedqvist una obligación fiscal en concepto de impuesto al valor agregado.

Hedqvist pretendía dedicarse a ofrecer servicios de intercambio de bitcoins por coronas suecas. La Ley del IVA sueca eximía del impuesto a las operaciones relativas a billetes y monedas que sean medios legales de pago, con excepción de los objetos de colección, es decir, las monedas de oro, plata u otro metal, así como los billetes que no sean utilizados normalmente para su función de medio legal de pago o que revistan un interés numismático.

El Tribunal ponderó que una divisa virtual puede definirse como un tipo de moneda digital no regulada, emitida y verificada por sus creadores y aceptada por los miembros de una comunidad virtual concreta. La divisa virtual «bitcoin» forma parte de las divisas virtuales denominadas «de flujo bidireccional», que los usuarios pueden comprar y vender con arreglo al tipo de cambio. Por lo que respecta a su uso en el mundo real, estas divisas virtuales son análogas a las demás divisas intercambiables, y permiten adquirir bienes y servicios tanto reales como virtuales. Las divisas virtuales se distinguen del dinero electrónico, en la medida en que, a diferencia de éste dinero, en el caso de las divisas virtuales los fondos no se expresan en la unidad de cuenta tradicional, por ejemplo, en euros, sino en una unidad de cuenta virtual, como el «bitcoin» [\[1832\]](#).

Se señaló que la intención de Hedqvist era realizar operaciones electrónicamente, a través del sitio de Internet de su sociedad. Esta sociedad adquiriría unidades de la divisa virtual «bitcoin» directamente a particulares y empresas, o bien en una bolsa de intercambio internacional, y luego las revendería después en dicha bolsa de intercambio o las almacenaría. La sociedad del Sr. Hedqvist vendería también tales unidades a particulares o

empresas que realizasen pedidos en su sitio de Internet. En el supuesto de que el cliente hubiese aceptado el precio en coronas suecas propuesto por la sociedad del Sr. Hedqvist y se hubiera recibido el pago, las unidades de la divisa virtual «bitcoin» vendidas se enviarían automáticamente a la dirección «bitcoin» indicada. Las unidades de la divisa virtual «bitcoin» vendidas por esa sociedad serían, bien las adquiridas por ella directamente en la bolsa de intercambio después de que el cliente hubiera efectuado su pedido, bien las que ya tuviera almacenadas. El precio propuesto por dicha sociedad a los clientes se determinaría en función del precio vigente en una bolsa de intercambio específica, añadiéndole cierto porcentaje. La diferencia entre el precio de compra y el precio de venta sería el beneficio de la sociedad del Sr. Hedqvist. Esta sociedad no facturaría otros gastos [\[1833\]](#).

El Tribunal consideró:

“..la divisa virtual de flujo bidireccional «bitcoin», que se intercambiará por divisas tradicionales en las operaciones de cambio, **no puede calificarse de «bien corporal»** en el sentido del artículo 14 de la Directiva del IVA, puesto que, (...) **no tiene ninguna finalidad distinta de la de ser un medio de pago** (...) Lo mismo ocurre con las divisas tradicionales, dado que se trata de monedas que son medios de pago legales (...) Por lo que respecta, en segundo lugar, al carácter oneroso de la prestación de servicios (...) una prestación de servicios sólo se efectúa «a título oneroso» (...) si existe una relación directa entre el servicio prestado y la contraprestación recibida por el sujeto pasivo (...) Tal relación directa se establece cuando existe entre quien efectúa la prestación y su destinatario una relación jurídica en cuyo marco se intercambian prestaciones recíprocas y la retribución percibida por quien efectúa la prestación constituye el contravalor efectivo del servicio prestado al destinatario (...) entre la sociedad del Sr. Hedqvist y quienes contraten con ella **existiría una relación jurídica sinalagmática** en la que las partes en la operación se comprometerían recíprocamente a entregar ciertos importes en

una determinada divisa y a recibir su contravalor en una divisa virtual de flujo bidireccional, o viceversa. También se indica allí que, por su prestación de servicios, **esta sociedad recibiría una contrapartida equivalente al margen incluido por ella en el cálculo de los tipos de cambio** a los que estaría dispuesta a vender y comprar las divisas en cuestión (...) unas operaciones como las controvertidas en el litigio principal **constituyen prestaciones de servicios realizadas a cambio de una contrapartida** que presente una relación directa con el servicio prestado, es decir, prestaciones de servicios a título oneroso (...) **constituyen prestaciones de servicios realizadas a título oneroso** (...) operaciones como las controvertidas en el litigio principal, consistentes en un intercambio de divisas tradicionales por unidades de la divisa virtual «bitcoin», y viceversa, y realizadas a cambio del pago de un importe equivalente al margen constituido por la diferencia entre, por una parte, el precio al que el operador de que se trate compre las divisas y, por otra, el precio al que las venda a sus clientes (...) las operaciones exentas del IVA en virtud de estas disposiciones son, por su naturaleza, operaciones financieras, si bien no han de ser realizadas necesariamente por bancos o establecimientos financieros (...) Al ser la divisa virtual «bitcoin» un medio de pago contractual, por una parte, no es posible considerarla ni una cuenta corriente ni un depósito de fondos, un pago o un giro. Por otra parte, a diferencia de los créditos, cheques y otros efectos comerciales (...) constituye un medio de pago directo entre los operadores que la aceptan (...) operaciones como las controvertidas en el litigio principal no están incluidas en el ámbito de aplicación de las exenciones establecidas en esa disposición (...) las operaciones relativas a divisas no tradicionales, es decir, a divisas distintas a las monedas que son medios legales de pago en uno o varios países, **constituyen operaciones financieras siempre que tales divisas hayan sido aceptadas por las partes de una transacción como medio de pago alternativo a los medios legales de pago** y no tengan ninguna finalidad distinta de la de ser un medio de pago (...)

debe interpretarse en el sentido de que **constituyen operaciones exentas del IVA** con arreglo a dicha disposición unas prestaciones de servicios como las controvertidas en el litigio principal, consistentes en un intercambio de divisas tradicionales por unidades de la divisa virtual «bitcoin», y viceversa, y realizadas a cambio del pago de un importe equivalente al margen constituido por la diferencia entre, por una parte, el precio al que el operador de que se trate compre las divisas y, por otra, el precio al que las venda a sus clientes. [\[1834\]](#)» (el resaltado es mío).

4.7.6. *La responsabilidad por riesgo: la teoría del riesgo creado* [\[1835\]](#)

Ossola y Azar señalan que la noción de riesgo connota a causas o eventos que previsiblemente pueden provocar un daño, a la materialización de esos peligros en un contexto determinado, y a las consecuencias perjudiciales de contingencias previstas o imprevistas [\[1836\]](#).

Señalan los autores que el *riesgo* fundamenta a las siguientes figuras jurídicas:

- i) los riesgos en tanto vicios de la cosa, que son contingencias que la destruyen o la tornan impropia para un fin determinado;
- ii) los riesgos del contrato y cómo distribuirlos ante la ruptura de la economía contractual;
- iii) los riesgos de la empresa que afectan a un establecimiento empresarial y que no son trasladables a sus empleados;
- iv) el riesgo de la *prestación*, que refiere a la incidencia que tiene cierta utilidad prevista como resultado de una obligación de resultado;
- v) el riesgo de una cosa riesgosa, entendido como la calidad previsible, probable y ordinaria que tiene un objeto dado para dañar a otros en función

de su uso o actuación;

vi) el riesgo de la actividad, que incluye específicamente el diseño, organización y administración de un sistema informático; y

vii) el riesgo de desarrollo, que hace referencia al riesgo que nace por la utilización de productos elaborados cuyo riesgo es conocido *ex post facto* que el bien es puesto en el mercado [\[1837\]](#).

4.7.6.1. *El riesgo como factor de atribución de responsabilidad*

La noción de riesgo, presente en los siete supuestos arriba identificados, refiere a un evento o calidad con potencialidad previsible de producir pérdidas, y que es un mecanismo de imputación de consecuencias jurídicas [\[1838\]](#).

En lo que nos interesa, se centrará el análisis en los supuestos de riesgos de la prestación, de la cosa riesgosa, y de la actividad. En éstos tres supuestos, el *riesgo* opera como un factor de atribución o *imputación objetiva* de la responsabilidad emergente por la afectación de un interés del acreedor de una obligación de resultado, o por la producción de un daño causado por cosas o actividades *riesgosas* [\[1839\]](#). En cambio, en el caso puntual del riesgo de desarrollo, si el productor o fabricante efectivamente ignoraba el riesgo al momento de lanzar al mercado el producto o servicio, el riesgo puede funcionar como una defensa y eximición de responsabilidad del responsable, como una causa de justificación; *a contrario sensu*, si el riesgo era conocido, el riesgo opera como factor objetivo de atribución e imputación [\[1840\]](#). Así, la atribución de un riesgo es una operación de imputación, entendida como la imposición de la consencuencia resarcitoria en contra del sujeto que ocupaba la situación objetiva descrita en la norma –propiedad, guarda o ejercicio–, y que presupone la relación causal entre la actuación de la cosa o actividad, con el daño [\[1841\]](#).

Esta atribución de responsabilidad implica que el Derecho considera que el riesgo determina un juicio de responsabilidad, atribuyéndose el daño

producido o a producirse al sujeto que crea, soporta, contribuye o se aprovecha de la situación de riesgo, prescindiéndose de todo reproche subjetivo de culpabilidad del agente [\[1842\]](#).

4.7.7. *Fundamento de la responsabilidad por riesgo*

Ossola y Azar puntualizan que el riesgo define una responsabilidad objetiva en el art. 1757, CCCN [\[1843\]](#), en la que la culpa o el error de conducta son irrelevantes para liberar de la imputación, sin que tampoco pueda liberarse por el cumplimiento de técnicas de prevención, y cuyas únicas eximentes son la causa ajena prevista en el art. 1722, CCCN [\[1844\]](#) y las previstas en el art. 1758, CCCN [\[1845\]](#).

Ahora bien, afirman los autores citados que la potencialidad dañosa de una actividad requiere un fundamento idóneo que permita *convertirla* en causa de imputación. A tal fin, existen cinco teorías.

La teoría del riesgo creado postula que toda actividad que crea para los demás un riesgo especial hace al autor, a quien la puso en existencia o a quien la realiza, responsable por los eventuales daños que pueda causar a terceros, independientemente del error de conducta que pueda (o no) existir. Esta teoría es el fundamento del art. 1758, CCCN [\[1846\]](#).

Una segunda teoría, llamada del provecho o del riesgo-beneficio, postula que dónde se encuentre la ganancia, allí corresponde también imponer las cargas. Así, todo aquel que saca provecho o beneficio de una actividad, asume también los costos que ella provoca, incluidos los daños que pueda producir. En esta teoría, el damnificado está obligado a acreditar la obtención de la utilidad, y no basta con identificar a la actividad fuente del daño [\[1847\]](#). Esta teoría también está receptada explícitamente, en el art. 1758, CCCN.

Una tercera teoría, es la del riesgo de la empresa o riesgo profesional, cuyo fundamento es análogo al de la teoría del riesgo-beneficio. En el CCCN, el riesgo profesional justifica la atribución de responsabilidad al franquiciante

por defectos del sistema, salvo culpa o dolo del franquiciado, conforme al art. 1521 ^[1848], y también al proveedor en una relación de consumo por las cosas y servicios riesgosos cuya utilización suponga un riesgo para la salud física de los consumidores –art. 6, Ley N° 24.240 ^[1849].

La cuarta teoría, es la del riesgo anormal o excepcional. Se trata de contingencias notablemente peligrosas, o que escapan a los parámetros de normalidad común. Esta teoría se aplica para identificar actividades que introducen peligros o riesgos excepcionales, para consagrar regímenes diferenciados o de responsabilidad agravada, como ocurre con la actividad nuclear y la utilización de material radioactivo, y en general con la generación, manipulación, transporte, tratamiento y disposición final de residuos peligrosos y daños nucleares ^[1850].

Finalmente, la quinta teoría es la de los riesgos de la cosa y de actividades riesgosas, términos que son considerados sinónimos y son receptados por el Art. 1757, CCCN ^[1851]. Se requiere en estos casos que la actividad *per se* sea riesgosa. Según el texto legal, la actividad será riesgosa por su naturaleza, por los medios empleados o por las circunstancias de su realización.

Así, sostienen Ossola y Azar que “la solución pasa por reconocer que la calificación legal de riesgosa a una actividad exige verificar esa calidad como inherente a ella. En otras palabras, se trata de un riesgo característico o previsible. Lo característico apunta a una tipificación legal o reglamentaria vigente que asigne esa entidad a una determinada actividad.” ^[1852] Concluyen los autores citados que los parámetros fijados por la ley impiden presumir la peligrosidad de la actividad y requieren que ella sea efectivamente establecida.

4.7.8. Actividades riesgosas

El origen del término es el Código Civil italiano, en su art. 2050, a donde, según Galgano, citado por Ossola y Azar, “actividad peligrosa es la actividad caracterizada por notable potencialidad del daño; por una peligrosidad

intrínseca o de todos modos dependiente de la modalidad del ejercicio y de los medios de trabajo empleados. [\[1853\]](#)»

Como se adelantó, una actividad será (o no) riesgosa o peligrosa por su naturaleza, por los medios empleados o por las circunstancias de su realización [\[1854\]](#). Ossola y Azar sostienen que el uso de ambos vocablos no es accidental, ni cabe afirmar que sean sinónimos.

En el derecho argentino, lo peligroso alude a un riesgo calificado, que presume una declaración en tal sentido, como ocurre con ciertas tareas riesgosas o insalubres, en el art. 168, Ley N° 20.744 [\[1855\]](#), y que diferencia tal riesgo de otro considerado normal u ordinario [\[1856\]](#). Por ello, la incorporación de la calidad de *riesgoso* en el art. 1757, CCCN importa ampliar el concepto más agravado de lo *peligroso* a situaciones con potencialidad objetiva y abstracta de daño [\[1857\]](#). Sin embargo, afirman los autores citados que la calidad de peligroso o riesgoso no es un *numerus clausus*, ni requiere la calificación normativa para ser reconocida.

De tal modo, la actividad podrá ser intrínsecamente riesgosa por su propia naturaleza, como por ejemplo, los bancos de sangre, hemoderivados y hemodiálisis, que contienen riesgos ínsitos de transmisión de virus y enfermedades, y por ello en casos de contagios, no es necesario acreditar el vicio o la contaminación de la sangre que la transmite, tal como exige la imputación objetiva del riesgo o vicio de la cosa, sino la ejecución o la exposición a la actividad peligrosa en sí misma [\[1858\]](#).

La actividad también podrá ser riesgosa por los medios empleados, o por las circunstancias de su realización. En el primer caso, “la actividad es riesgosa o peligrosa por los medios empleados cuando normalmente es inocua, pero adquiere aquella cualidad porque una persona hace uso de mecanismos, instrumentos, aparatos o sustancias que son peligrosos por la velocidad que desarrollan, por su naturaleza explosiva o inflamable, por la energía que contienen, por el lugar anómalo en que se encuentran o por otras causas análogas, o bien si han sido los medios utilizados los que han aumentado la

probabilidad de riesgo. [\[1859\]](#)»

En punto a las circunstancias de su realización, son aquellas que “*pese a no revestir ordinariamente un peligro regular o constante, las modalidades de tiempo, modo y lugar la tornan especialmente peligrosa. Por ejemplo, el trabajo en la construcción o en la obra.*” [\[1860\]](#)»

4.7.9. Beneficiario de la actividad riesgosa

Para el CCCN, en su art. 1758, el sindicado como responsable por una actividad riesgosa es quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros, excepto lo dispuesto en la legislación especial [\[1861\]](#).

Se apunta que si bien la norma designa legitimados pasivos de modo alternativo, ello no implica la exclusión de unos por los otros, ya que son todos codeudores de una obligación concurrente. El servirse de la actividad identifica como legitimado pasivo a quien, sin realizar la actividad materialmente, utiliza la acción de un tercero que en definitiva la ejecuta, e.g., subcontrataciones, delegaciones, intermediaciones, dependencias económicas y funcionales entre quien encarga o se sirve, y el agente, dependiente o delegado que la realiza [\[1862\]](#). El obtener provecho alude al riesgo-beneficio, justificante de la imposición de las consecuencias a quien extrae una utilidad de la actividad.

Finalmente, las exclusiones legales a las que refiere el art. 1758 son aquéllos regímenes especiales que amplían o reducen los legitimados pasivos, como ocurre en la Ley N° 25.675 de medioambiente, N° 23.184 de espectáculos públicos, N° 24.804 de actividad nuclear, N° 24.240, de defensa del consumidor y del usuario, e incluso el propio CCCN, en su art. 1762:

“Actividad peligrosa de un grupo. Si un grupo realiza una actividad peligrosa para terceros, todos sus integrantes responden solidariamente por el daño causado por uno o más de sus miembros. Sólo se libera quien demuestra que no

integraba el grupo.”

4.7.10. Eximentes de responsabilidad

Afirman Ossola y Azar que, dada la responsabilidad objetiva asociada a actividades riesgosas o peligrosas, los legitimados pasivos se liberan probando la causa ajena [\[1863\]](#), pero, además, se prevén ciertos eximentes especiales. Así, el uso de la cosa contrario a la voluntad expresa o presunta de su dueño o guardián, lo liberará:

Art. 1758.- Sujetos responsables. El dueño y el guardián son responsables concurrentes del daño causado por las cosas. Se considera guardián a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella. El dueño y el guardián no responden si prueban que la cosa fue usada en contra de su voluntad expresa o presunta.

En caso de actividad riesgosa o peligrosa responde quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros, excepto lo dispuesto por la legislación especial.”

Repárese, sin embargo, que el término *cosa* empleado en el primer párrafo del art. 1758 no incluye bienes inmateriales, tales como la información y los programas de computación o la red de Internet [\[1864\]](#), por tanto, el uso de la cosa en contra de la voluntad de su dueño o guardián no se aplicará en casos que involucren software, y, además, no está prevista para las actividades riesgosas o peligrosas [\[1865\]](#).

Por otro lado, el art. 1757 declara expresamente que tanto la autorización administrativa para la realización de una actividad riesgosa como el cumplimiento de técnicas de prevención es ineficaz para eximir de responsabilidad el titular de la actividad riesgosa [\[1866\]](#).

Por tanto, la ajenidad de la causa dañina será la única forma de liberar al titular de la actividad riesgosa, pero la forma de *operar* de la causa ajena requiere algunas precisiones.

En rigor, la causa ajena *excluye* la responsabilidad porque *rompe* el nexo causal, tanto en materia de responsabilidad objetiva como también de responsabilidad subjetiva ^[1867]. Al no haber autoría ni imputación posible, es lógicamente impredicable postular la presencia de un factor de atribución ^[1868], toda vez que la causalidad es un elemento *previo* a determinar, pues la asignación de un factor de atribución a una conducta presupone que la conducta existió, y que tiene conexión causal con el daño.

De lo expuesto surge que el orden lógico de análisis debe siempre ser: (1) determinar si existe (o no) relación causal, cuya eximente es la causa ajena en sus tres manifestaciones: (i) caso fortuito o fuerza mayor, (ii) hecho de la víctima y (iii) hecho de un tercero por quien no se debe responder; (2) determinar si la conducta causalmente vinculada es, además, antijurídica, cuya eximente son las causas de justificación, y sin perjuicio de que existan casos de responsabilidad por actos lícitos; y (3) asignar un factor de atribución, objetivo o subjetivo. Si la conducta es lícita, pero igual se debe responder, ello ocurrirá por equidad o por garantía, pero no por el riesgo, suponiendo los autores citados que éste siempre supone licitud ^[1869].

Por lo anterior, se preguntan Ossola y Azar si los factores objetivos de atribución, como la actividad riesgosa, tienen o no eximentes *propios*, siendo que la *causa ajena* opera, en realidad, rompiendo el vínculo causal ^[1870].

4.8. *Primeras reflexiones preliminares en torno a la responsabilidad civil en entornos de blockchain*

En este Capítulo hemos pasado apretada revista a la teoría de la conexidad contractual que rige en el mundo no digital, comprendiendo en muchos casos a contratos electrónicos. Se ha puntualizado la flexibilización del principio del efecto relativo de los contratos en *entornos de red off-chain*, y sus impactos en

términos de incumplimientos contractuales cruzados, frustración de la finalidad económica común y extensión de responsabilidades.

Luego, nos hemos adentrado en el estudio de algunos contratos que, desde la periferia o en el interior mismo del entorno *blockchain*, permiten que los usuarios ingresen al entorno *blockchain* a través de *Exchanges* y *Wallets*, adquiriendo o recibiendo tokens digitales en ICOs, STOs, *air drops* o comprando o vendiendo bitcoins.

Se han puntualizado algunos aspectos controvertidos del contrato de programación de un *Smart Contract*, y se ha remarcado la importancia que las *Specs* tienen en toda obra de arquitectura y desarrollo de software –i.e., un documento técnico y complejo que equivale a una fusión por absorción de los clásicos planos de planta, vistas, cortes, volumetrías, cálculo estructural, al esquema de instalaciones eléctricas y sanitarias, al proyecto de ascensores, al proyecto de bomberos, o al proyecto de calefacción que arquitectos e ingenieros desarrollan para construir una obra física.

También se han resaltado los procesos propios de la auditoría de software, que verifican que no existan errores en la programación de acuerdo a las *Specs*, y la importancia que tal auditoría adquiere cuando un contrato inteligente se despliega en una *blockchain* para *operar tal como se lo programó, sin injerencia humana*.

Se han analizado las particularidades de los *Exchanges* y las *Wallets*, con foco en los riesgos inherentes y específicos de esta nueva actividad. Se han remarcado aspectos de KYC & AML, los innumerables casos de monedas sospechosas y listras negras, y los ciberataques más célebres. Se han visto también los primeros casos *fáciles* y también uno no tan fácil, como es el *leading case Quoine*, primero en su especie.

Se han abordado las diferencias en las formas de licenciar el software, y cómo el software *open source* plantea un enfoque muy distinto al software propietario, donde la gratuidad en el acceso al software “*as is*” viene condicionada por la aceptación de cláusulas de limitación de responsabilidad, que muy probablemente serían consideradas abusivas si hubiera un pago de licencia.

También se han analizado los primeros pasos del BCRA en materia de

billeteras electrónicas, remarcándose como el *Open Banking* comienza a ganar espacio regulatorio a nivel global, a la par que el uso de criptoactivos crece y va, también, desarrollándose la *Blockchain 2.0* y sus usos, convirtiendo y transformando lenta pero constantemente a la *Internet de la Información* en una *Internet del Valor*. Recordemos también cómo de a poco el *Legal Design* se ofrece y gana espacios como un mecanismo novedoso de simplificación de esta compleja realidad contractual (y conexas), y se postula como un nuevo modo de exposición de la información legal centrado en el usuario de la misma.

En este periplo, hemos también abordado la álgida cuestión de la responsabilidad civil en entornos de *blockchain*, analizando posturas europeas y norteamericanas que tienen, cada una en su medida, muy fuertes y convincentes argumentos.

Así, se ha postulado como el Derecho Privado deberá abordar la nueva *Internet del Valor* sin reglas claras ni muchas leyes específicas, dependiendo, en gran medida, de organismos reguladores y Jueces para moldear el uso y la distribución de riesgos en entornos de *blockchain*.

Se ha visto como la Corte Suprema de la India controla los abusos reglamentarios de el Banco Central del país, o como el Tribunal Europeo de Justicia aclara posiciones en materia fiscal. Se ha visto también la importancia de un regulador comprometido con la protección del inversor –SEC, CFTC–, y, finalmente, se ha conceptualizado a grandes líneas la responsabilidad objetiva, la responsabilidad por riesgo creado, su fundamento como factor de atribución de responsabilidad, y se han dado algunas precisiones sobre sus eximentes.

Toca ahora tratar de unir todos estos puntos, para intentar dar alguna pauta que guíe la resolución de los casos *difíciles e importantes*. Los casos fáciles, se sabe, se resuelven con las normas y *principios* que ya existen. Pero los casos difíciles, pueden exigir el desarrollo de *nuevas normas y nuevos principios*, o la flexibilización de las existentes.

Al finalizar este apartado se ha incluido una visualización de la red contractual on-chain.

4.8.1. Los Usuarios de la Innovación y los Creadores de la Innovación

En una Economía post-COVID-19 fuertemente digitalizada por *necesidad*, es evidente que los *Usuarios* de la *Innovación* se han multiplicado exponencialmente.

Tenían antes el derecho a participar de la innovación, pero sólo hizo falta una pandemia para que ese derecho se convierta, en muchos casos, en una *obligación* de usar la innovación. El cúmulo de “Covid-apps” diseñadas desde el sector público para el control sanitario de la población demuestran el punto, e incluso demuestran que la privacidad *cede* en casos de salud pública, incluso en las regiones más celosas de la privacidad, como es la Unión Europea.

Algo similar ocurre con los usuarios de *blockchain*, quienes por ahora voluntariamente deciden entrar al entorno, a través de alguna de sus funcionalidades, normalmente la de criptoactivos, pero esto no es óbice a tantos otros usos “no financieros” de la cadena de bloques que van ganando *momentum*, como por caso la *SSID*, o la trazabilidad de información de partes, alimentos y piezas, o incluso la emisión del voto en *blockchain*. Quizás, la primera *imposición* de ingreso al entorno *blockchain* vendrá de China, con el despliegue del Yuan Digital para pagar salarios públicos. Pero, por ahora, el ingreso y uso de la *blockchain* y de sus funcionalidades, sigue estando reservado a la libre y voluntaria iniciativa particular de usuarios individuales o corporativos.

Ahora bien, lo que hoy es voluntario, es posible que sea obligatorio en el futuro *no muy distante*. Digamos, 2030. La *obligatoriedad* no devendrá tanto por la imposición del sector público –al estilo Chino–, como por la conveniencia y masificación del uso de la cadena de bloques para resolver problemas que antes se resolvían de otro modo.

Del mismo modo que hoy nadie obliga a otra persona a usar Internet, pero la practicidad de enviar un e-mail impone su uso, y desplaza al correo tradicional, que queda reservado para resolver *otro tipo* de problemas. En el futuro *no muy distante*, probablemente nadie pueda obligar efectivamente a nadie a utilizar *blockchain*, pero habrá ámbitos en los cuales su utilización por

conveniencia la volverá, *de facto*, una tecnología de uso obligado. Cuánto tiempo deberá pasar para llegar a ese estadio, es hoy un dato incierto, aunque coincido con GARTNER cuando estima que a partir de 2025, otras tecnologías como IoT, IA y SSID se combinarán con las plataformas de *blockchain*, permitiendo microtransacciones entre objetos autónomos y computarizados, sin intervención humana y la utilización creciente de DAOs, dando lugar a la llamada era del *enhanced-blockchain*.

Pues bien, el Derecho debe estar preparado para cuando ese momento llegue, pero también, el Derecho debe ser *creado e interpretado* para que ese momento *pueda llegar*. De otro modo, los *Usuarios* de la *Innovación* verían afectado su derecho de *usar* una nueva tecnología, y se afectaría también a los impulsores privados de la *Innovación*, las empresas, empresarios y emprendedores *honestos* que crean y promueven nuevas formas de hacer las cosas, y asumen riesgos –a veces muy grandes– de desarrollo para permitir que los *Usuarios* accedan, usen y se beneficien, de la *Innovación*.

A no dudar: la *Innovación* es y será siempre una actividad *riesgosa*, pero los riesgos de la *Innovación* deben también sopesarse contra los problemas que la *Innovación* resuelve, contra las nuevas formas de valor que se crean o se crearán, y, en última instancia, contra el valor social neto generado por *arriesgarse a innovar*.

Con este particular encuadre, si se quiere, de Política Pública de Innovación, se intentará ahora unir todos los puntos abordados en este Capítulo, postulando y afirmando que el *Usuario* de la *Innovación*, al igual que *Creador* de la *Innovación*, asumen riesgos distintos que aquéllos riesgos asumidos por quienes no innovan y prefieren seguir resolviendo problemas del mismo modo en que se lo viene haciendo. El *Usuario* de la *Innovación* nunca será *Amante* del *Status Quo*. Y mucho menos, el *Creador* de la *Innovación*.

4.8.2. *Redes contractuales dentro de redes digitales*

Sin dudas, la teoría de la conexidad contractual jugará un rol trascendente en *blockchain*, donde es posible detectar redes de contratos coligados

operando, incluso de manera automática vía *Smart Contracts*, dentro de una red descentralizada.

Recuérdese aquí que los contratos conexos pueden ser celebrados por adhesión a cláusulas generales, pueden ser contratos de consumo, o pueden también ser contratos paritarios. Sólo en éste último caso, sus cláusulas serán para sus partes la ley misma. En los otros dos, i.e. consumo y adhesión, las cláusulas del contrato –cualquiera sea la especie contractual: licencia, servicios, compraventa, comisión, mandato, corretaje, etc.– podrán o deberán ser interpretadas y, en su caso, modificadas de acuerdo a las normas que rigen los conflictos y riesgos del consumo y de la contratación adhesiva, teniéndose en cuenta que en ésta última, puede incluirse tanto a un usuario final, como a un empresario que contrata con una gran empresa predisponente, para abastecer su proceso empresarial, sea cuál fuere éste.

En este sentido, más arriba he afirmado que la celebración de un contrato inteligente *on-chain* puede normalmente ser un caso de conexidad contractual, ya que pueden concurrir los siguientes contratos coligados entre sí: (i) el contrato convencional subyacente que puede prever los términos y condiciones a ser programados en un *Smart Contract* de ejecución o de garantía; (ii) el contrato de desarrollo de software para implementar una *blockchain* privada, incluyendo el contrato de licencia para su uso; (iii) el contrato de licencia de uso de una *blockchain open source* pública; (iv) el contrato de compra o venta de criptomonedas a un *Exchange*, y de custodia de llaves con una *Wallet*; (v) el contrato de compra de tokens, tengan éstos fines funcionales –utility token– o de inversión –security token–, incluso de inversión *derivada*, si el token deriva su valor de un activo subyacente o del resultado de inversiones automatizadas, si se tratase de DAICOs; y (vi) de licencia de uso de *Smart Contracts* ya desarrollados, o de desarrollo y programación de un *Smart Contracts* a medida, incluyendo los servicios de auditoría técnica sobre el código de programación, en su caso.

Hasta tanto la conexidad sea declarada expresamente por una ley, se aplicarán quizás los criterios jurisprudenciales de conexidad *off-chain* a la conexidad *on-chain*, con mayores o menores ajustes y adaptaciones, y en casos fáciles, difíciles o importantes. Al resolver éstos últimos, y al aplicarse criterios previos no pensados para nuevas realidades, el Juez, intérprete de los hechos y del Derecho, no debiera olvidar lo expuesto más arriba, que será

varias veces repetido: (i) la *Innovación* es y será siempre una actividad *riesgosa*; los riesgos de la *Innovación* deben sopesarse contra los problemas que se resuelven, contra las nuevas formas de valor que se crean o se crearán, y, en última instancia, contra el valor social neto generado por *arriesgarse a innovar*; y (ii) el *Usuario* de la *Innovación*, al igual que *Creador* de la *Innovación*, *asumen riesgos* distintos que aquéllos riesgos asumidos por quienes no innovan y prefieren seguir resolviendo problemas del mismo modo en que se lo venía haciendo. A dónde debe trazarse la línea divisoria de los riesgos que puede y *debe* soportar el *Usuario* de la *Innovación*, y de los riesgos que puede y *debe* soportar el *Creador* de la *Innovación*, deberá fijarse atendiendo a las circunstancias de modo, tiempo y lugar de cada caso concreto, y nunca –salvo casos fáciles de evidente *strepitus fori*, e.g., normas AML y de protección del usuario contra fraudes– debiera fijarse por ley, si no se quiere inhibir la *Creación* de *Innovación*.

4.8.3. *Responsabilidad objetiva, seguros y cláusulas de limitaciones de responsabilidad en entornos blockchain*

Siendo la *Innovación* una actividad riesgosa *per se*, es lógico aplicar un criterio de responsabilidad objetiva en cabeza de su *Creador*, puesto que *Usuario* acepta el riesgo de la *Innovación* en tanto y en cuanto ésta cumpla su promesa de resolver algún problema de un modo más eficiente que el que ofrece el estado del Arte y *Status Quo ex ante*. Ese resultado útil se derivará del uso de distintas innovaciones concatenadas, en el entorno *blockchain*, yo las llamo *Incremental On-Chain Innovations, Io-cl*, innovaciones intra-tecnológicas que ocurrirán en el entorno blockchain.

Cuando el *Usuario* pueda ser calificado de *Usuario final*, no le serán oponibles las cláusulas de exclusión de responsabilidad del *Creador*, pero el único recurso del *Usuario* debiera limitarse al seguro de responsabilidad civil que contrate el *Creador* –con más su propio patrimonio–, contratación ésta que debiera ser obligada, de modo de ampliar la posibilidad real de conseguir una indemnización de los daños y perjuicios *eventuales* y *contingentes*. Este criterio es idéntico al impuesto al fiduciario cuando el Art. 1685 CCCN lo obliga a tomar un seguro que cubra los daños eventuales, en beneficio de los beneficiarios. Los riesgos y montos cubiertos deberán ser razonables con los

riesgos *creados y asumidos* por los Usuarios de la Innovación.

Cuando el Usuario de la Innovación pueda ser calificado de empresario, el reparto y asignación de riesgos con el Creador de la Innovación podrá tener diseño exclusivamente contractual, a través de contratos paritarios o adhesivos, y podrán o no acordarse seguros adicionales.

4.8.4. *Taxonomía del token y asignación de riesgos*

Dentro del entorno *blockchain*, el *Usuario de la Innovación* podrá usar asset, utility o security tokens, pero sólo en éste último caso debiera el token cumplimentar las mismas normas que se exigen en todo el mundo para los mismos productos *off-chain* que resuelven el mismo problema, dada la equivalencia funcional desde el punto de vista del *problem-solution-fit*.

Tal equivalencia funcional derivará de las condiciones de creación del token, que normalmente estarán divulgadas y expresadas en un documento al que coloquialmente por convención se ha dado en llamar *White Paper*.

El Usuario de asset y utility tokens, por su parte, busca algo *distinto* que un producto de inversión, y cuando un *Usuario de la Innovación* adquiere asset tokens para transaccionar pagos digitales o como reserva de valor, o adquiere utility tokens para utilizar servicios y bienes digitales actuales o futuros, manifiesta su voluntad de asumir riesgos, también, *distintos*. *Distinto*, en el sentido empleado, no es sinónimo de *inferior*. En efecto, pre-financiar el producto digital comprando una ICO ofrecida por el Creador de la Innovación como modo de financiación de su desarrollo, no es un riesgo *menor* al que asume, por ejemplo, un comprador de un autoplan. Pero, lógicamente, se asume un conocimiento *distinto*, tanto en profundidad como en calidad, en el pretense Usuario de un token digital que en el comprador de un autoplan. Ese mayor conocimiento lo sitúa en una posición contractual particular, y le permite asumir un riesgo *distinto*, al cual no está, de ordinario, expuesto un comprador de autoplan. Lo anterior no significa que los Creadores de utility tokens no deban cumplir un estándar de información también agravado, a pesar de tener Usuarios calificados por su conocimiento o *expertise tecnológico*. Por el contrario, significa que deberán informarse todos los riesgos *distintos* de manera adecuada, de modo tal que el Usuario

pueda válida y voluntariamente decidir aceptarlos, en el caso que el Creador decida transferirlos al Usuario como condición de la contratación. Es en éste sentido que debe interpretarse la manda del Art. 1107, cuando dispone que el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, *para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos.*

4.8.5. Responsabilidad de los actores periféricos e internos: Exchanges, Wallets y desarrolladores de Smart Contracts

El rol de estos actores periféricos del entorno *blockchain*, que permiten el ingreso, permanencia y el egreso de *Usuarios* a y de la *Innovación*, es esencial para el desarrollo de la tecnología *blockchain*.

Asumen un gran riesgo, por cuanto alojan valor para terceros. Los casos de ciberataques glosados a lo largo de este Manual ilustran acabadamente el punto. Ahora bien, el riesgo que asumen es socialmente conveniente, por cuanto sin *Exchanges* y *Wallets* eficientes, los *Usuarios* no podrían ingresar ni permanecer en el entorno *blockchain*.

Así, del mismo modo que el desarrollo de la industria de la aeronavegación requirió –ya por mucho tiempo, quizás– una limitación expresa de la responsabilidad objetiva eventual por daños a terceros, acordada en el art. 11 del Convenio de Roma de 1952, ratificado por la Ley N° 17.404, quizás la nueva legislación que se dicte para regular el entorno *blockchain* deba también incluir algún tipo de limitación a la responsabilidad, de la mano con una obligación de tomar ciertos seguros. Es que, del mismo modo que ninguna aerolínea puede seriamente garantizar que un avión funcionará, en todos y cada uno de sus sistemas, de modo perfecto y seguro, ningún desarrollador de software podrá garantizar que su producto es *error-free*, ni siquiera auditado que sea, varias veces y por varios auditores.

Entonces, así como se limitó la responsabilidad del operador de aeronaves, debiera pensarse si no es conveniente, para impulsar su desarrollo, pensar un esquema de limitación de responsabilidad específico del desarrollador de *Smart Contracts*. Mientras ello no ocurra, se le aplicarán a los contratos de

desarrollo de software las mismas normas que se aplican a un contrato de obra y a las obligaciones de resultado, pero, debe reconocerse, la utilidad potencial que un software puede ofrecer a la Sociedad puede ser varias veces superior a la utilidad de una obra física, cuyos usuarios serán, por definición, un número acotado, determinado, o determinable. Sostener lo contrario implicará equiparar los riesgos y beneficios *sociales* de la construcción de un edificio, con los riesgos y beneficios sociales del uso masivo de WhatsApp, o de PayPal, o con los riesgos y beneficios que podrían generarse por el uso masivo de Libra y Calibra.

4.8.6. *Blockchains privadas y consorciadas*

Estos trazos gruesos sobre la eventual responsabilidad civil en entornos de *blockchain* estarían incompletos si no precisaran el *distinto* alcance y efecto de la responsabilidad en un entorno de *blockchain* privada o consorciada. Éstas arquitecturas de *blockchains* son muy distintas a la de una *blockchain* pública.

En las *blockchains* privadas es posible identificar fácilmente al o a los responsables de su operación y funcionamiento, y el uso de las mismas requiere de una licencia, de un permiso. Difícilmente en una *blockchain* privada o consorciada se utilicen licencias de *open software*. De hecho, será improbable que un desarrollo tecnológico privado de la complejidad que puede llegar a tener una *blockchain*, sea puesta a disposición de los Usuarios sin previamente aceptar una serie de condicionamientos contenidos en el licenciamiento que permite el acceso, la lectura, y la escritura de información en la misma. Los nodos que la creen y la mantengan podrán pactar las formas de asignar y distribuir entre ellos los riesgos, pero seguramente serán comunes las cláusulas de limitación de responsabilidad para los *Usuarios* de la *Innovación*. En tanto éstos no encuadren como Usuarios *finales*, podrían eventualmente disputar la eficacia de las limitaciones contractuales *ex post facto* y una vez acaecido el hecho dañoso, pero es previsible que dichas cláusulas sean oponibles y eficaces, por cuanto no han desnaturalizado una obligación del *Creador*, sino que han asignado y repartido los *riesgos de desarrollo* entre el *Creador* y el *Usuario*, debiéndose siempre recordar que no existe tal cosa como el software perfecto. Su actualización, revisión y corrección es tarea permanente, si el *Creador* es realmente un *honesto*

4.8.7. *Innovación y Competencia*

Finalmente, útil es recordar lo ya dicho: a toda (gran) innovación (casi) siempre le ha seguido un cambio (o, a veces, un terremoto) competitivo. Y si los mercados fueran perfectos, la *Innovación* y la *Competencia* siempre irían de la mano, por ser el modo en que la *eficiencia* lo indica. Pero lo contrario es lo que normalmente ocurre, y en los (imperfectos) mercados humanos, *Competencia* e *Innovación* suelen ir enfrentados, y pocas veces van bien coordinadas. Con carácter axiomático, puede nuevamente afirmarse que *sin competencia no hay necesidad de innovar* y, muchas veces ya nos ha enseñado la Historia, son las mismas *innovadoras* empresas –los mismísimos *Creadores* de la *Innovación*– que lideran nuevos mercados gracias a un conjunto de desarrollos tecnológicos propietarios, las que son permeables a abusar de su *market power* e intentan extenderlo a otros mercados donde no son líderes.

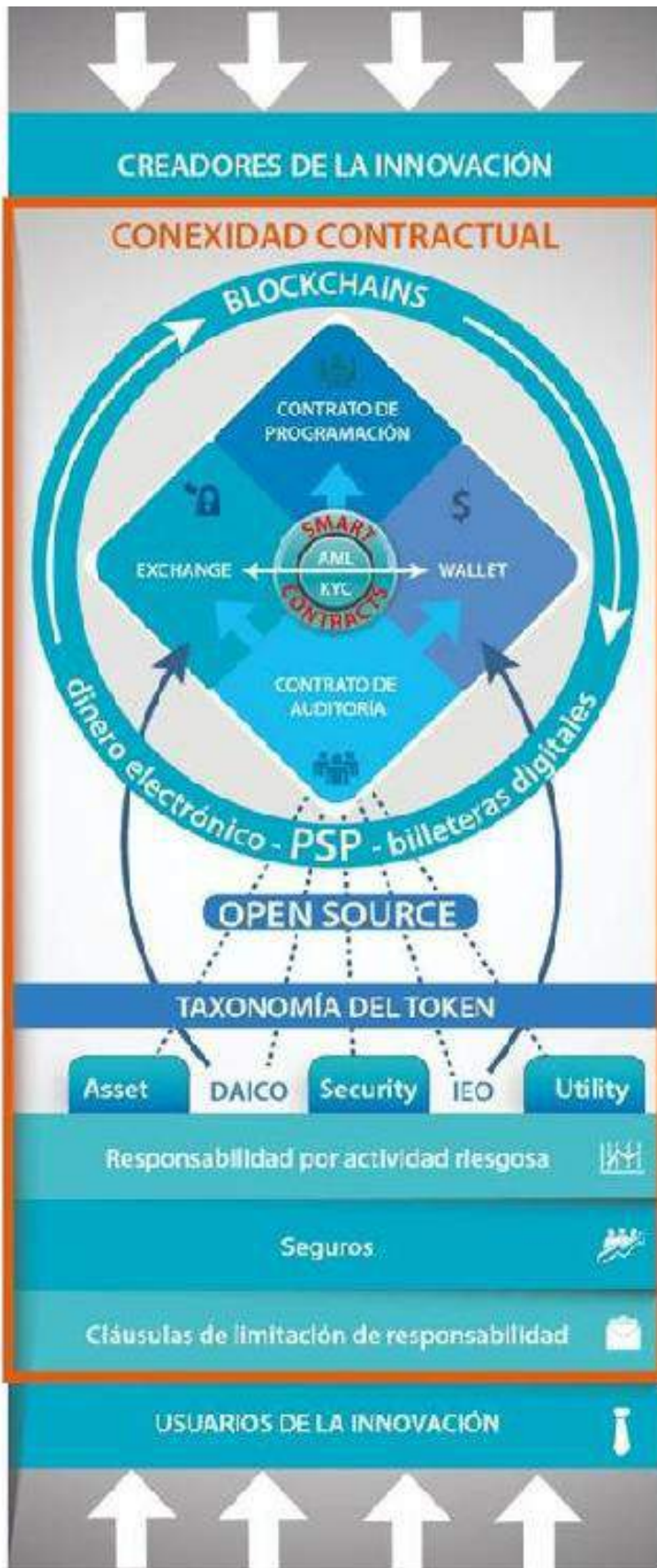
Reitero aquí mi poco científica opinión, ya que no poseo más evidencia que mi propia, subjetiva, y sesgada percepción personal: pareciera que abundan los abusos anticompetitivos cuando las empresas que lideran una tecnología comienzan a usufructuar la fase de uso masivo de la misma, e.g. Internet Explorer vs. Netscape. Aparecen allí los abusos tecnológicos de los (nuevos) líderes de (nuevos) mercados que son, muchas veces, verdaderos océanos azules reservados para unos pocos corsarios tecnológicos.

Es por lo anterior que, así como postulo que debe pensarse muy seriamente si conviene (o no) diagramar limitaciones de responsabilidad para promover el desarrollo de una tecnología –de modo tal que los *riesgos ilimitados* de una actividad *per se* riesgosa como es *innovar* no la inhiban ni la frenen–, deberá también pensarse en una actuación contundente, *deterrent-oriented*, y castigarse sin temor y con todo el peso de la Ley a los *Creadores* de la *Innovación* que infringan las normas de defensa de la competencia en entornos digitales, y abusen del poder de mercado que les ha conferido el haber asumido los riesgos inherentes a la *Innovación*. Puntualmente, donde se hayan construido posiciones de dominio tecnológico, no deberán aceptarse prácticas y conductas empresarias que:

- a) Fijen en forma directa o indirecta el precio de venta, o compra de bienes o servicios al que se ofrecen o demanden en el mercado, así como intercambiar información con el mismo objeto o efecto;
- b) Fijen, impongan o practiquen, directa o indirectamente, de cualquier forma, condiciones para (i) producir, procesar, distribuir, comprar o comercializar sólo una cantidad restringida o limitada de bienes, y/o (ii) prestar un número, volumen o frecuencia restringido o limitado de servicios;
- c) *Concerten la limitación o control del desarrollo técnico o las inversiones destinadas a la producción o comercialización de bienes y servicios;*
- d) *Impidan, dificulten u obstaculicen a terceras personas la entrada o permanencia en un mercado o excluirlas de éste;*
- e) Afecten mercados de bienes o servicios, mediante *acuerdos para limitar o controlar la investigación y el desarrollo tecnológico*, la producción de bienes o prestación de servicios, o para dificultar inversiones destinadas a la producción de bienes o servicios o su distribución;
- f) Subordinen la venta de un bien a la adquisición de otro o a la utilización de un servicio, o subordinar la prestación de un servicio a la utilización de otro o a la adquisición de un bien;
- g) Sujeten la compra o venta a la condición de no usar, adquirir, vender o abastecer bienes o servicios producidos, procesados, distribuidos o comercializados por un tercero;
- h) Impongan condiciones discriminatorias para la adquisición o enajenación de bienes o servicios sin razones fundadas en los usos y costumbres comerciales;
- i) Negarse injustificadamente a satisfacer pedidos concretos, para la compra o venta de bienes o servicios, efectuados en las condiciones vigentes en el mercado de que se trate;

- j) Suspender la provisión de un servicio monopólico dominante en el mercado a un prestatario de servicios públicos o de interés público;
- k) Enajenar bienes o prestar servicios a precios inferiores a su costo, sin razones fundadas en los usos y costumbres comerciales con la finalidad de desplazar la competencia en el mercado o de producir daños en la imagen o en el patrimonio o en el valor de las marcas de sus proveedores de bienes o servicios; y
- l) La participación simultánea de una persona humana en cargos ejecutivos relevantes o de director en dos o más empresas competidoras entre sí.

Cuadro de presentación analítica: Red Contractual *On-Chain**



CREADORES DE LA INNOVACIÓN

CONEXIDAD CONTRACTUAL

BLOCKCHAINS

CONTRATO DE PROGRAMACIÓN

EXCHANGE

WALLET

CONTRATO DE AUDITORIA

dinero electrónico - PSP - billeteras digitales

OPEN SOURCE

TAXONOMÍA DEL TOKEN

Asset

DAICO

Security

IEO

Utility

Responsabilidad por actividad riesgosa



Seguros



Cláusulas de limitación de responsabilidad



USUARIOS DE LA INNOVACIÓN



*El autor agradece la colaboración del D.I. Diego Germán Amaya.

V. Aspectos Regulatorios y Tributarios

5.1. Introducción. Primeros pasos hacia el entorno blockchain en Argentina

En este Capítulo V se realizará una valoración de ciertos aspectos regulatorios específicos a la *blockchain*, a los criptoactivos y a los contratos inteligentes, y se analizarán también los primeros avances en torno a la tributación de los mismos.

Una primera advertencia al lector. Así como la tecnología *blockchain* comienza lentamente a ser testada en industrias tan variadas como la salud, o la generación distribuida de energía o la distribución digital audiovisual, pasando por los mercados financieros y los registros públicos inmobiliarios, transaccionando información a través de contratos inteligentes, la perspectiva del regulador comienza también a ampliarse para incluir múltiples posibles reguladores, en algunas ocasiones con áreas de incumbencia muy específica, y en otras ocasiones, con superposición de poderes regulatorios entre sí. Sirve como ejemplo lo afirmado por el el Juez del caso *CFTC v. McDonnell*: hasta tanto la legislación no clarifique la materia, en EE.UU en materia de criptoactivos las opciones son “1. No regulation; 2. Partial regulation through criminal law prosecutions of Ponzi-like schemes by the Department of Justice, or state criminal agencies, or civil substantive suits based on allegations of fraud; 3. Regulation by the CFTC; 4. Regulation by the SEC; 5. Regulation by FinCEN; 6. Regulation by the IRS; 7. Regulation by private exchanges (self-regulation); 8. State regulations; y 9. A combination of any of the above.”

En Argentina, la primera definición regulatoria vino en 2014 por parte de la Unidad de Información Financiera al abordar los payment tokens y su relación con las normas de KYC-AML ^[1871]. Luego, en Diciembre de 2017, la Comisión Nacional de Valores emitió una advertencia al público inversor, definiendo a la *blockchain* y a los tokens, y alertando sobre el riesgo de fraude

y de ofertas públicas irregulares de posibles títulos valores regulados [\[1872\]](#). También en Diciembre de 2017, cuando el *cryptomarket* se acercaba a su máximo histórico de Enero de 2018 y llamaba la atención de todas las agencias fiscales del mundo, llegó la primera regulación impositiva de los criptoactivos, impulsada por la Administración Federal de Ingresos Públicos, al incluir las monedas digitales en la Ley N° 27.430 de reforma del Impuesto a las Ganancias, publicada en el Boletín Oficial el 29 de Diciembre de 2017.

A principios de 2019, se ha conformado la Mesa de Innovación Financiera del Banco Central de la República Argentina (“MIF”), que se presenta como una forma de colaboración entre los bancos, las empresas Fintech y el organismo regulador. La dinámica consiste en que los participantes formen parte de las políticas y las conozcan *antes* de su implementación para lograr una transición más fluida.

La MIF define el concepto de Fintech como *innovaciones financieras posibilitadas por el avance tecnológico que acarrearán efectos concretos en la provisión de servicios financieros a través de la transformación de modelos de negocios, aplicaciones, procesos o productos* [\[1873\]](#), y reconoce que constituye un verdadero desafío para el regulador, ya que debe identificar y controlar los riesgos creados por la transformación innovadora del sistema financiero, sin sofocar los beneficios generados por la eficiencia y la competencia.

La MIF ha definido cuatro grupos de trabajo: (1) Medios e Infraestructura de Pagos; (2) *Soluciones Blockchain*; (3) Tecnologías y Sistemas Transversales; y (4) Canales Alternativos de Crédito y Ahorro.

Bueno es saberlo, ya desde el año 2016, el BCRA ha impulsado las competencias de innovación financiera, con la primera edición del *#HackatonFinanciero*. Allí se dieron cita creativa más de 400 concursantes y un equipo interdisciplinario de 100 mentores.

Los *Hackatones*, así como formatos de los nuevos formatos de *Sprints & Scrums*, ofician de aceleradora de ideas, aglutinando durante dos días a diseñadores, programadores, estudiantes, profesionales, economistas y emprendedores, trabajando para vincular ideas innovadoras con soluciones concretas con foco en la inclusión financiera, la transformación financiera,

oportunidades de financiamiento y las metas de inflación. Ya se presentaban por aquel Hackatón de 2016 “ideas locas”, como propuestas para la tokenización del Peso [\[1874\]](#). China, en ese mismo momento (2016), ya llevaba más de dos años de investigación en tándem con las mayores empresas de tecnología para tokenizar el Yuan [\[1875\]](#), la primera CBDC.

Otra iniciativa muy fructífera del BCRA ha sido el *Programa de Innovación Financiera* lanzado en 2017, que ha incluido la celebración de Jornadas Federales en las capitales de provincias. Ya desde 2018, las bases del programa convocan a proyectos del entorno *blockchain* [\[1876\]](#), y en 2019 se comenzó a convocar específicamente proyectos enfocados a *RegTech* para el BCRA y la CNV [\[1877\]](#).

En todos los casos, hay premios en moneda *fiat* para los primeros tres proyectos; en 2019 el estímulo total a repartir fue equivalente a 6.000 Dólares. Esto podría cambiarse, quizás, para ampliar el foco: 1 bitcoin a repartir entre los primeros tres.

En Abril de 2020, el BCRA anunció que viene trabajando en un piloto de *blockchain* que combina contratos inteligentes al implementar un sistema descentralizado de gestión de los reclamos por los débitos directos en cuenta que son rechazados por los clientes de las entidades financieras [\[1878\]](#).

La CNV, por su parte, también ha creado en 2019 un *Task Force Fintech CNV* que funciona de manera coordinada con la Mesa de Innovación Financiera [\[1879\]](#), y que trabaja cuatro ejes: P2P Lending, *SandBox* regulatorio, *Blockchain* y *Criptoactivos* y, por último, Género y Fintech [\[1880\]](#), con el objetivo de un espacio de diálogo entre los reguladores y los nuevos emprendimientos del ecosistema fintech local.

Ahora bien, excepto por la tangencial referencia legislativa del Congreso de la Nación a los fines estrictamente impositivos, la *blockchain*, los criptoactivos y los contratos inteligentes aún no han ingresado al tratamiento del Honorable Congreso de la Nación, y como se dijo antes [\[1881\]](#), es

competencia del Congreso la regulación del dinero electrónico y similares [\[1882\]](#).

Ahora bien, en general, el entorno *blockchain* entendido como un sistema descentralizado, una tecnología distribuida y una red contractual, espera a nivel global –al menos hace diez años– un posicionamiento legislativo claro, permisivo o prohibitivo, que permita *prever* la asignación y una distribución más eficiente de los *riesgos creados*, y aumentar la inclusión financiera y la digitalización –harto necesaria en países como Argentina.

Se ha visto que hay países que avanzan más rápido que otros, o incluso, sub-regiones dentro de esos países, como el cantón de Zug, o los Estados de Wyoming y Delaware, o países como Singapur y Japón.

Argentina puede (y debe) jugar un papel central en el entorno *blockchain*, ya que tiene el talento humano, y le sobran los problemas para solucionar en materia de inclusión y transformación financiera, oportunidades de financiamiento y metas de inflación. Considero sin temor a errar que todos éstos problemas pueden ser eficientemente resueltos en *blockchain*.

5.2. Breve descripción de los mercados de dinero fiduciario regulados en Argentina

5.2.1. Bancos, compañías financieras y proveedores no financieros de crédito

Eduardo Barreria Delfino afirma que toda razón que la dinámica de la economía real y de los circuitos de la producción, la comercialización, el consumo y la inversión presentan altibajos temporales en la fluidez de los flujos de cobros y pagos que se generan continuamente [\[1883\]](#). Ello conduce a la necesidad de mecanismos que posibiliten la transferencia de recursos de sujetos económicos con *superávit* de liquidez hacia sujetos económicos con *déficit* de liquidez. Tal función de acercamiento la desarrollan agentes especializados autorizados para operar en los mercados que integran el

sistema financiero, que actúan bajo la supervisión estatal que busca prevenir desequilibrios, disfunciones o malas conductas de tales agentes, con miras a cuidar el ahorro de los ciudadanos y permitir satisfacer las necesidades de financiación de todos los sectores de la sociedad [\[1884\]](#).

Es dentro del sistema financiero así creado que se posibilita el comportamiento del ahorro y la inversión a la par que se facilitan pagos e intercambios en el sistema económico. El correcto funcionamiento de este sistema requiere un equilibrio en la gestión de la intermediación financiera, sin perturbaciones o turbulencias en los flujos de recursos transables.

Ahora bien, evidentemente la creación de *nuevos recursos transables digitales* puede trastocar el funcionamiento del sistema financiero, al colocar una nueva forma de valor distinta al dinero fiduciario, y que también genera sus propios flujos de liquidez y déficit, dando lugar al nacimiento de *nuevos* mercados digitales donde tales flujos se encuentran e interactúan. Tales nuevos recursos digitales surgen al margen de las instituciones autorizadas para intermediar en el mercado monetario, o para contactar en el mercado de capitales, quienes han sido –hasta ahora– los únicos encargados de resolver los descalces temporales entre inversión y repago que representan necesidades de financiación tanto de gobiernos, como de empresas e individuos.

Dentro del sistema financiero, el sub-sistema bancario está conformado por intermediarios financieros autorizados para actuar conforme a la Ley N° 21.526, y se encuentra bajo la supervisión permanente del BCRA, quien está encargado de preservar el valor de la moneda, y, consecuentemente, actuar como regulador monetario y supervisar el funcionamiento del mercado y de sus agentes [\[1885\]](#), además de ejecutar la política cambiaria [\[1886\]](#).

La función del sub-sistema bancario es atraer, administrar y canalizar las ofertas y demandas de recursos financieros, sea para financiar el consumo de las personas o el capital de trabajo de las empresas [\[1887\]](#), dando lugar a la banca de consumo y a la banca comercial. El sub-sistema bancario está integrado por entidades bancarias –banca comercial, de inversión e hipotecaria– y también por entidades no bancarias, e.g., compañías

financieras, sociedades de ahorro y préstamo y cajas de crédito. Los bancos tienen la capacidad, además, crear medios de pago ^[1888]. Es evidente el rol clave de los bancos, al canalizar el ahorro hacia quienes invierten o producen.

El BCRA monopoliza la emisión monetaria de dinero *fiduciario*, o de curso legal. Su función esencial, además de controlar al sub-sistema bancario, es la de administrar la política monetaria *vis-à-vis* los objetivos macroeconómicos de estabilidad, través de los encajes, el nivel de liquidez y los tipos de interés de corto plazo ^[1889]. Un banco central controla la totalidad de la masa monetaria de un país, y por definición, mira a un horizonte temporal de largo plazo. Éste *largo* plazo pocas veces es entendido por la política –cuyo horizonte temporal es 2 y 4 años–, de allí que se afirma (muy) sabio despolitizar la política monetaria ^[1890]. Cuando la política se apropia de la política monetaria, se obtiene, tarde o temprano, una moneda generalmente (muy) débil. Así, se ha probado que los países con bancos centrales independientes tienen menores tasas de inflación ^[1891].

La Constitución Nacional delega en el Congreso de la Nación las atribuciones de establecer y reglamentar *un banco federal* con facultad de emitir moneda, así como otros bancos nacionales; hacer sellado de la moneda, fijar su valor y el de las extranjeras para toda la Nación; proveer a lo conducente para la prosperidad del país y a la defensa del valor de la moneda –C.N., arts. 75, incs. 6, 11, 18 y 19–.

El art. 126 de la Constitución Nacional, a su turno, le prohíbe a las provincias acuñar moneda o autorizar bancos con facultades de emitir billetes sin autorización del Congreso. La soberanía monetaria ha sido delegada por las provincias a la Nación ^[1892]. Así, la Ley N° 12.155 del año 1935 creó el Banco Central de la República Argentina ^[1893]. En 1992 se sancionaría la Ley N° 24.144 que aprobó la nueva carta orgánica del BCRA, convirtiéndolo en un organismo autárquico, y prohibiéndole *expresamente* en el Art. 3: (i) que, en la formulación y ejecución de la política monetaria y financiera, el BCRA estuviera sujeto a *órdenes, indicaciones o instrucciones* del Poder Ejecutivo Nacional; y (ii) asumir obligaciones de cualquier naturaleza que impliquen

condicionar, restringir o delegar sin autorización expresa del Honorable Congreso de la Nación, el ejercicio de sus facultades legales.

Sin que deba extrañarnos, pues ya estamos acostumbrado al movimiento pendular argentino, no es bueno –desde lo institucional– que deba permanecer cubierto por un silencio cómplice tremenda negligencia cometida por la Ley N° 26.739, de 2012, que modificó el Art. 3 de la carta orgánica del BCRA, que le asignaba desde 1992 como única misión primaria y fundamental la de preservar el *valor de la moneda*.

En Argentina, desde 2012, el BCRA debe promover, en la medida de sus facultades y *en el marco de las políticas establecidas por el gobierno nacional*, la estabilidad monetaria, la estabilidad financiera, el empleo y el desarrollo económico con equidad social, pero *no debe velar por el valor de la moneda*. Así, desde 2009 a 2019 la inflación en Argentina superó el 700%, y en los últimos 100 años la tasa promedio de inflación anual fue del 105% [\[1894\]](#). Adivine, lector, la razón.

En cuanto a los bancos que el BCRA debe regular, afirma Barreira Delfino que el control sobre la banca es intenso, ya que la vida económica y financiera de un país depende de las entidades financieras para canalizar los medios de pagos –banca transaccional– y para canalizar el ahorro y la inversión –banca crediticia– [\[1895\]](#).

Los bancos juegan un rol muy importante al intermediar entre depositantes de fondos excedentes y prestatarios previo análisis de riesgo y crédito [\[1896\]](#). Así, la supervisión bancaria apunta a prevenir que los depositantes pierdan sus depósitos, y que tal pérdida, si ocurre, se expanda en el sistema bancario –riesgo sistémico–.

Dentro del BCRA, la Superintendencia de Entidades Financieras y Cambiarias fue puesta a cargo de la supervisión de la actividad financiera y cambiaria en todo el país en 1992, pero veinte años después, en 2012 [\[1897\]](#), se le quitó a dicha Superintendencia el carácter de órgano desconcentrado, quedando sometida a la voluntad política del Directorio del BCRA. Como se vió, la misma Superintendencia controla también a los PSPs.

La intermediación financiera habitual de recursos financieros y las entidades que pueden realizarla están reguladas en la Ley N° 21.526. La intermediación financiera se entiende como la realización masiva de actos de adquisición y correlativa transferencia de derechos sobre recursos financieros [\[1898\]](#), y si bien *no es* un servicio público y puede ser realizada por todos los habitantes de la Nación, su ejercicio está fuertemente regulado por las Leyes N° 21.526, por el CCCN [\[1899\]](#), por la carta orgánica del BCRA y las reglamentaciones por éste emitidas.

La Ley N° 21.526 tipifica en su art. 2 a los distintos tipos de intermediarios financieros: bancos comerciales, bancos de inversión, bancos hipotecarios, compañías financieras, sociedades de ahorro y préstamo para la vivienda u otros inmuebles, y cajas de crédito. La enumeración no es taxativa [\[1900\]](#). Cada una de las categorías reconocidas pueden realizar las operaciones financieras que en cada caso se regulan, aunque la tendencia global es hacia la banca *universal*, donde los bancos pueden realizar todas las operaciones activas, pasivas y de servicios que no estén expresamente prohibidas, sosteniéndose que la banca integrada se encuentra menos expuesta al riesgo *vis-à-vis* la banca especializada [\[1901\]](#). En este tema tan sensible, no estoy tan convencido que la banca universal realmente tenga menor exposición al riesgo. En efecto, postulo que en EE.UU. la derogación –en 1999– de la Ley *Glass Steagall* –sancionada en respuesta al crack del '29 y su durísima crisis financiera–, que prohibía a los bancos comerciales ser, a la vez, bancos de inversión, fue la semilla que 8 años después causó la crisis de las hipotecas *subprime*, que luego se globalizaría [\[1902\]](#).

En Mayo de 2020, el sistema financiero regulado por el BCRA está compuesto por 15 compañías financieras, 50 entidades financieras –entre extranjeras y nacionales–, 13 bancos públicos, a las que se suman 118 empresas no financieras emisoras de tarjeta de créditos, 39 sociedades de garantía recíproca, 22 casas de cambio, más de 200 agencias de cambio y más de 260 proveedores no financieros de crédito [\[1903\]](#).

5.2.2. Algunas innovaciones jurídicas en la financiación del capital de trabajo: el cheque y el pagaré bursátil. El cheque electrónico y la factura de crédito electrónica

5.2.2.1. La negociación bursátil de cheques de pago diferido [\[1904\]](#)

En la hazañosa búsqueda empresaria por el financiamiento en Argentina, ya en 2010 se consolidaba un hito muy criollo: la negociación bursátil de cheques de pago diferido (CHPD).

Efectivamente, a poco más de un lustro desde su permisión en 2005, la negociación bursátil de CHPD se había convertido en 2010 [\[1905\]](#) en una herramienta tan útil como atractiva a la hora de conseguir financiamiento para el sector pequeño y mediano (PyMEs).

Sin dudas, fue una innovación jurídica muy relevante, cuyos efectos perduran. El CHPD es una orden de pago, librada a fecha determinada posterior que no exceda en 360 días a la fecha de su libramiento, contra una entidad autorizada en la cual el librador a la fecha de vencimiento debe tener fondos suficientes depositados a su orden en cuenta corriente o autorización para girar en descubierto [\[1906\]](#).

Ahora bien, la necesidad cotidiana de fondos, frecuentemente lleva a que el tenedor de un CHPD no pueda esperar a su vencimiento para el cobro del mismo. Así, más comúnmente el sector PyME, se recurre al descuento del CHPD para obtener el valor presente de un monto futuro prometido a determinada fecha.

En orden a normar dicho proceder fundado en una innegable necesidad empresaria, en Noviembre de 2001 se introdujo una modificación a las normas sobre transmisión de los cheques [\[1907\]](#). Ello permitió el descuento bancario de CHPD. *Id quod plerumque accidit*, las tasas (de descuento) cobradas por las entidades financieras no hacían del todo conveniente la operatoria.

Luego de noviembre, llegó Diciembre de 2001. A no dudarlo, la actualización del potencial "riesgo sistémico" repercutió en todos los ámbitos de la vida económica, pero más agudamente impactó en el segmento PyMEs. Justamente, la fuerte restricción al acceso al crédito llevó a la necesidad de pensar *nuevas* alternativas de financiamiento.

En ese contexto, se dicta el Decreto 386, publicado en el Boletín Oficial el 15 de julio de 2003. El mismo autoriza la *negociación bursátil* de CHPD en las Bolsas de Comercio, en procura de una reducción "significativa" de las tasas de interés, a la par que permite la negociación en un ámbito institucionalizado [\[1908\]](#) y transparente.^[1]_[SEP]

El régimen creado por el Dto. 386/03 establece como Autoridad de Aplicación a la Comisión Nacional de Valores (CNV), cuya función principal consiste en regular y supervisar la negociación bursátil de CHPD. En ejercicio de tal encargo, la CNV dictó la Resolución General 452 en octubre de 2003, estableciendo las modalidades posibles de negociación, las que en aquél momento debían ser reglamentadas, además, por las Bolsas y Mercados. A su vez, el Banco Central de la República Argentina debía reglamentar los aspectos relativos al CHPD [\[1909\]](#).

A su turno, la Bolsa de Comercio de Buenos Aires (BCBA) emitió la Resolución 2/2003 reglamentando la cotización de los CHPD y lo propio hizo la Bolsa de Comercio de Córdoba [\[1910\]](#). Por su parte, Mercado de Valores S.A. (Merval) habilitó la negociación de CHPD, y a su turno lo hizo el Mercado de Valores de Córdoba S.A [\[1911\]](#). Finalmente, Caja de Valores S.A. emitió su Reglamento Operativo de Cheques de Pago Diferido.

La CNV en su momento ha regulado la negociación bursátil de CHPD en base a los siguientes principios: (i) Igualdad de acceso al inversor: CNV dispuso que la negociación de CHPD disponga de un sistema de interferencia de ofertas con prioridad precio-tiempo, como modo de garantizar la igualdad de acceso al inversor; (ii) *numerus clausus* de operatorias admitidas: CNV previó, originalmente, dos operatorias pasibles de ser realizadas con CHPD sujetas, en aquél momento, a la reglamentación de las Bolsas y Mercados. Sin

embargo, dejó abierta la puerta para autorizar en el futuro otras modalidades de negociación, siempre y cuando se aprobasen los procedimientos de análisis de riesgo crediticio propuestos por las entidades autorreguladas ^[1912]; y (iii) Controles delegados en Bolsas y Mercados: fueron puestas, en aquel momento, en cabeza de las Bolsas y Mercados ciertas obligaciones de control. Concretamente, estaban obligados a verificar que los CHPD en ellos negociados no presenten defectos formales. Asimismo, debían verificar la legitimación de los firmantes y la autenticidad de las firmas asentadas en los CHPD.

Las modalidades de negociación utilizadas por aquél entonces eran la negociación patrocinada y la negociación avalada. En la primera modalidad, la libradora ^[1913] de los CHPD solicitaba la autorización a una Bolsa de Comercio para que los beneficiarios de sus cheques puedan ofrecerlos a la negociación bursátil. ^[SEP] En la segunda, en cambio, era una Sociedad de Garantía Recíproca (SGR) o una entidad financiera la que solicitaba a una Bolsa de Comercio la autorización para cotizar CHPD avalados o bien los certificados de CHPD avalados emitidos por las entidades financieras.

Evidentemente, el uso del descuento bursátil de cheques *avalados* se impuso en volumen, al reducirse el riesgo del inversor por el aval de una SGR. Por ejemplo, en Mayo de 2019 según datos del Mercado Argentino de Valores (MAV) el volumen negociado de cheques de pago diferido alcanzó los 9.646 millones de Pesos, lo que implicó un crecimiento interanual del 276% ^[1914]; sobre dicho monto, un 32% correspondió al segmento patrocinado, y el saldo al segmento de cheques avalados.

Las SGR o las entidades financieras debían cumplir lo reglamentado respecto de las libradoras, y podían las Bolsas fijar un monto máximo de CHPD avalados por SGR susceptibles de ser negociados. El aval prestado por una SGR debía constar en el CHPD y la Bolsas exigían a dichas sociedades la comunicación fehaciente al otorgar un aval a un CHPD que será negociado en un Mercado de Valores.

La principal ventaja del descuento bursátil de un CHPD era y es el menor costo financiero soportado por el anticipo de los fondos, toda vez que las tasas

bursátiles de descuento son menores que las bancarias.

En adición, el descuento bursátil no castigaba ni castiga el límite crediticio del librador respecto de su banco (lo que sí acontece si descuenta CHPD ante la entidad financiera con la que tiene acordado un determinado límite de asistencia crediticia), lo que redundaba en una ampliación del monto de financiamiento del emisor del CHPD.

Finalmente, existía una ventaja impositiva de no tributar el impuesto al débito y crédito bancario, lo que es también un elemento sumamente positivo. A ello se sumaba y se suma el prestigio y seriedad de una empresa que ha recurrido al mercado de capitales para financiarse, que se acrecientan de un modo palpable. Ello puede mejorar -en combinación con otros aspectos- su posición como unidad receptora de inversión.

En enero de 2020, CNV informaba que los instrumentos PyME acapararon el 25% del financiamiento (\$ 13.215 millones negociados en cheques de pago diferido), siendo los CHPD el instrumento más dinámico con una variación interanual de 163% ^[1915] . [SEP]

5.2.2.2. El pagaré bursátil ^[1916]

El éxito de la operatoria de descuento bursátil de CHPD entre los años 2003 y 2015 fue muy significativo, pero tenía como límite infranqueable el plazo máximo de libramiento de un cheque de pago diferido. Por ende, podía materializar un descuento de cuentas por cobrar, i.e., anticipar un flujo de corto plazo para financiar el capital de trabajo, pero no permitía vehiculizar la financiación de inversiones a más de 1 año.

Así, en 2016 se produjo otra segunda *innovación jurídica* en término de instrumentos de financiamiento, el *pagaré bursátil*. El primer día de Agosto de 2016 fue publicada en el Boletín Oficial la Ley N° 27.264, que lleva por título formal el de "Programa de Recuperación Productiva", y por título informal el de "*Ley PYME*".

A través de 57 artículos de fondo y mediante la modificación de ocho leyes nacionales ^[1917], la Ley PYME irradió importantes reformas en materia

tributaria [\[1918\]](#), creó un régimen transitorio de estímulo a la inversión productiva, creó un Registro de Empresas MiPyMES, un Registro de Consultores MiPyME y un Consejo de Monitoreo y Competitividad para la Micro, Pequeña y Mediana Empresa, y extendió todos los beneficios especiales para Micro, Pequeñas y Medianas Empresas a los contratos asociativos y cooperativas, creó una Red de Agencias de Desarrollo Productivo, y fomentó y estimuló la inversión para capacitación del personal de MiPyMEs [\[1919\]](#).

La ley también dio un nuevo rumbo al Fondo Nacional de Desarrollo para la Micro, Pequeña y Mediana Empresa (el FONAPYME) y al Fondo de Garantía para la Micro, Pequeña y Mediana Empresa (el FOGAPYME) — cuyos comités de inversiones y de administración, respectivamente, pasaron a ser presididos por el Ministro de Producción—, siendo claro el espíritu de la ley de *facilitar* el acceso al financiamiento de Micro, Pequeñas y Medianas empresas, y promover la articulación e integración con las Provincias y los Municipios [\[1920\]](#).

Finalmente, se producen importantes modificaciones al régimen de Sociedades de Garantía Recíproca —cuya autoridad de aplicación será también el Ministerio de Producción—, agravándose sensiblemente el régimen sancionatorio, y modificándose también el régimen legal de Obligaciones Negociables y Letra de Cambio y Pagaré, con el fin de facilitar el financiamiento de MiPyMEs, obligándose además a las aseguradoras a invertir en instrumentos con oferta pública emitidos por Micro, Medianas y Pequeñas Empresas [\[1921\]](#).

Téngase en cuenta la Ley N° 26.831 de Mercado de Capitales declara entre sus principios fundamentales el de *promover el acceso de las pequeñas y medianas empresas al mercado de capitales*, facultando a la Comisión Nacional de Valores (CNV) a reducir o eximir las tasas de fiscalización y control y los aranceles de autorización en relación a emisiones efectuadas por pequeñas y medianas empresas, incluyendo a las cooperativas y mutuales.

Asimismo, la Ley N° 26.831, del año 2012, autorizó a la CNV a exceptuar a

las pequeñas y medianas empresas de la obligación de constituir el Comité de Auditoría, aunque deberán contar con al menos un síndico titular y un síndico suplente [\[1922\]](#). Téngase también en cuenta que las Normas de la CNV, T.O. 2013 contemplan una regulación específica para las emisoras PYME, entendiéndose por tales aquellas empresas cuyos ingresos totales anuales en Pesos no superan los umbrales fijados periódicamente por CNV [\[1923\]](#).

Así, presentándose un formulario con carácter de declaración jurada, una PYME puede acceder al Régimen PYME-CNV, y en caso de ser admitida, podrá operar bajo el Régimen PYME por 24 meses contados desde que completó la presentación de documentación necesaria para una emisión, y podrá emitir valores negociables representativos de deuda por hasta \$200.000.000,00 [\[1924\]](#), importe por hasta el cual CNV puede autorizar la creación de programas globales de emisión.

Debe destacarse que la Ley N° 27.264 expande sustancialmente el campo del Régimen PYME-CNV, al modificar la Ley N° 23.576 de Obligaciones Negociables y permitir a las Sociedades de Responsabilidad Limitada emitir obligaciones negociables en paridad con las Sociedades Anónimas, y autorizar expresamente a las Sociedades de Garantía Recíproca y a fondos de garantía (como el FOGAPYME) a avalar estas emisiones de "deuda PYME".

Las Normas de la CNV disponen que las emisiones bajo Régimen PYME sólo pueden ser adquiridas por inversores calificados, y que los Mercados autorizados pueden emitir dictámenes de precalificación no vinculantes respecto de la emisión que pretendan enmarcar en el Régimen PYME [\[1925\]](#). Estos dictámenes de precalificación informan sobre la capacidad financiera de la empresa, la evolución del patrimonio neto en los últimos tres años, un flujo de fondos proyectado a 18 meses, las principales características de la actividad de la emisora, su impacto en la economía local y el cumplimiento de los requisitos propios del Régimen PYME, *detallándose los antecedentes empresariales de los socios y la factibilidad técnica, financiera y económica respecto de la emisión.*

Finalmente, el régimen informativo que asumen los emisores PYME se materializa en la redacción de un prospecto de emisión debidamente aprobado [\[1926\]](#), y en el cumplimiento del "Régimen Informativo Periódico" a CNV [\[1927\]](#).

Detallada a grandes rasgos la Ley PYME, veamos ahora el pagaré bursátil, cuya primera operación en Argentina tuvo lugar en 2015 [\[1928\]](#).

La regulación del pagaré está contenida en el art. 1836, CCCN y en las Normas de la CNV que reglamentan este instrumento de financiación en el Título VI, Capítulo V, Sección XV [\[1929\]](#).

Con el fin de impulsar y promover la utilización del pagaré bursátil, la Ley PYME introduce importantes modificaciones en los arts. 44, 101 y 103 del Decreto-Ley N° 5.965/63, que permiten: (1) Emitir pagarés bursátil cuya amortización prevea el pago del capital con vencimientos sucesivos *en cuotas*, estipulando que la falta de pago de una o más cuotas faculta al acreedor a tener por caducos los plazos y exigir el pago total del capital; (2) Fijar, de manera supletoria, que el tipo de cambio aplicable a pagarés librados en moneda extranjera será el tipo de cambio vendedor informado por el Banco Nación al cierre del día anterior al del vencimiento de cada cuota o al vencimiento del pagaré; y (3) Incorporada la leyenda "para su negociación en mercados de valores", la oferta primaria y la negociación secundaria de pagarés bursátiles no se considerarán oferta pública en los términos del art. 2 de la Ley N° 26.831, y no requerirán autorización previa [\[1930\]](#), y el lugar de pago del pagaré será el domicilio del agente de depósito colectivo.

En enero de 2020, CNV informaba que se habían negociado \$195 millones a través de pagarés avalados [\[1931\]](#).

5.2.2.3. *El cheque electrónico* [\[1932\]](#) *y la factura de crédito electrónica*

Las más recientes innovaciones en materia de financiamiento PyME han

sido el cheque electrónico y la factura de crédito electrónica.

Ambos instrumentos fueron creados por la Ley N° 27.440, conocida como *Ley de Financiamiento Productivo* publicada en el Boletín Oficial el 11 de Mayo de 2018. El art. 216 de esta ley previó que el Poder Ejecutivo Nacional debería, dentro de los 90 días de promulgación, reglamentar un sistema de cheques electrónicos, de uso voluntario por el cuentacorrentista. Siguiendo tal mandato, aunque con alguna demora, el BCRA dictó el 28 de Junio de 2019 tres Comunicaciones: “A” 6725, 6726, y 6727, que vienen a regular el *E-CHEQ*. Se trata de un título valor cartular “*desmaterializado*”.

La Comunicación “A” 6725 modificó 32 puntos atinentes a la Reglamentación de la cuenta corriente bancaria contenida en las Circulares OPASI 2 – 569 y RUNOR 1- 1472, y tipificada en el art. 1393 CCCN. Los puntos más sobresalientes de la regulación general de los ECHEQs son los siguientes:

- (i) las normas del cheque común o de pago diferido se aplican supletoriamente a los ECHEQs en caso de vacío normativo, y siempre y cuando tales normas no sean incompatibles con la regulación del ECHEQ;
- (ii) en cuanto al registro de firmas, el cuentacorrentista deberá aceptar por escrito los elementos de seguridad del ECHEQ, obligarse a resguardarlos, y a reconocer y no repudiar todo ECHEQ librado mediante el uso de esos elementos, salvo que proceda un motivo de rechazo de ECHEQs, que son taxativamente los listados en la Sección 6 de la Comunicación, aunque disminuye *significativamente* el potencial rechazo del cheque por motivos formales como exceso de endosos, falta de un firmante adicional, o la posibilidad material de sustracción del formulario;
- (iii) el requisito de la firma quedará satisfecho si se utiliza *cualquier método electrónico que asegure indubitablemente la exteriorización de la voluntad del librador y la integridad del instrumento*, la confiabilidad de la operación de emisión y su autenticación en su conjunto, siempre y cuando el mismo haya

sido previamente aceptado por el titular de la cuenta corriente mediante la suscripción de un acuerdo con la entidad financiera donde opera con cuenta corriente, que establezca que no podrá desconocer las órdenes cursadas conforme dicho mecanismo y que las asumirá como propias;

(iv) los ECHEQ podrán ser endosados y/o avalados en forma electrónica, siempre y cuando se utilicen para ello mecanismos que cumplan lo requerido en el párrafo precedente, con la particularidad que no hay límite de endoso para el ECHEQ –siendo éste límite de 1 o 2 endosos, según se trata de cheque común o de pago diferido, respectivamente;

(v) cuando el librador, el beneficiario, el endosante, o persona habilitada a obrar en su representación, dé una orden de no pagar un ECHEQ invocando su adulteración –incluyendo su emisión apócrifa– se aplicarán las disposiciones sobre extravío, sustracción o adulteración, y, adicionalmente, se suspenderá la posibilidad de librar nuevos ECHEQ o endosarlos hasta dar cumplimiento a la obligación de presentar constancia de haber denunciado el hecho como delito. Sólo cuando la entidad financiera cuente con dicha constancia, y habiendo previamente analizado que las circunstancias del caso no ameritan mantener la suspensión, podrá autorizar al cuentacorrentista a librar y/o endosar nuevos ECHEQ;

(vi) el tenedor legitimado podrá efectuar la presentación al cobro de cada ECHEQ a partir de la correspondiente fecha de pago a través de una orden electrónica de acreditación o bien cobrarlo por ventanilla y, ante su rechazo, podrá requerir el correspondiente certificado en la entidad financiera depositaria o girada –según corresponda–, que deberá emitirlo conforme a lo establecido en Comunicación “A” 6727, la norma específica dictada al efecto;

(vii) en cuanto a las obligaciones del librador de ECHEQs, deberá dar aviso a la entidad financiera cuando se detecte adulteración o emisión apócrifa; y custodiar los elementos de

seguridad convenidos para el libramiento, visualización y/o gestión de ECHEQ, impidiendo su uso por personas o en condiciones no autorizadas; emplear los elementos de seguridad y procedimientos convenidos para el libramiento, gestión y depósito de ECHEQ únicamente para librarlos, depositarlos y/o gestionarlos conforme a las normas y acuerdos aplicables; no desconocer el ECHEQ librado mediante el uso de los elementos y procedimientos de seguridad convenidos para ello y no desconocer el depósito u operación realizada con un ECHEQ que sea efectuada mediante el uso de los elementos y procedimientos de seguridad convenidos para ello; y

(viii) la entidad en la cual el cuentacorrentista opere, deberá asegurar que el ECHEQ sea librado sin defectos formales y conforme a los mecanismos de seguridad convenidos; velar por el correcto funcionamiento de los mecanismos de seguridad convenidos para el libramiento y/o gestión de ECHEQ y por los datos de estos, impidiendo su uso por personas o en condiciones no autorizadas; transmitir al repositorio en forma íntegra los ECHEQ y todas las novedades relacionadas con ellos, empleando los procedimientos y medios establecidos al efecto e imprimir los certificados para acciones civiles de ECHEQ rechazados y entregarlos al tenedor legitimado o su representante debidamente acreditado, a su requerimiento, guardando la constancia de entrega y, en su caso, de la personería del receptor.

La Comunicación “A” 6726, por su parte, modificó la Circular SINAP 1 – 87, que reglamenta el sistema nacional de pagos, cheques, y otros instrumentos compensables. Esta reglamentación es de obligado cumplimiento para el/los administrador/es del Sistema de Almacenamiento; las entidades financieras; y las Infraestructuras de Mercado Financiero Gestoras y/o que realicen la custodia/registro de ECHEQs para su negociación bursátil, autorizadas conforme lo disponga el BCRA, las que deben adherir al “*ACUERDO SOBRE TRUNCAMIENTO, GENERACIÓN Y GESTIÓN ELECTRÓNICA DE CHEQUES Y OTROS DOCUMENTOS*”

COMPENSABLES” que se adjunta a la Comunicación, asumiendo por la suscripción una serie de obligaciones que se derivan de la actividad de gestión y/o custodia/registro de ECHEQs. En esta órbita regulatoria se inscribe la negociación bursátil de cheques de pago diferido, que, naturalmente, también podrá realizarse mediante ECHEQs.

En los casos de la negociación de un ECHEQ u otro documento electrónico compensable, las entidades gestoras de ECHEQs deberán remitir la información requerida al sistema de almacenamiento, siendo su exclusiva responsabilidad la integridad y validez de los datos proporcionados respecto del último tenedor legitimado y/o en su caso los avales existentes, para el tramo de negociación avalada.

Finalmente, la Comunicación “A” 6727 modificó la Circular SINAP 1 – 88, que también reglamentaba el sistema nacional de pagos, cheques, y otros instrumentos compensables.

Esta tercera Comunicación reguló la emisión de certificaciones necesarias para iniciar acciones civiles contra quien corresponda, y dispone que si por cualquier motivo un ECHEQ no fuese pagado, total o parcialmente, la entidad financiera depositaria deberá emitir, ante el requerimiento del beneficiario, la Certificación para ejercer Acciones Civiles (CAC) establecida en el art. 61 de la Ley N° 24.452 y sus modificatorias.

En el caso de cobro por ventanilla, la entidad girada será la responsable de dicha función. *La expedición de esta certificación bloqueará el registro del ECHEQ en el Sistema de almacenamiento de cheques generados por medios electrónicos*, su emisión será en soporte papel, sin medidas de seguridad especiales y deberá estar firmada por dos funcionarios autorizados de la entidad financiera al pie del documento, con todas sus fojas inicializadas.

A fin de poder consultar la concordancia de lo expuesto en la CAC con los datos del sistema de almacenamiento de cheques por parte de los funcionarios judiciales, endosantes, avalistas o terceros, que hayan accedido al documento, cada CAC contará con un “Código de Visualización” para verificar la información a través de una página de internet.

Esta página de internet para la consulta centralizada de la CAC a través de su código de visualización será implementada por la Cámara Electrónica de

Compensación de Bajo Valor (CEC-BV) que tiene el mandato de operar y administrar el sistema de almacenamiento de los ECHEQ.

Para ello, la CEC-BV *deberá implementar un sistema de almacenamiento de los ECHEQ para registrar libramientos y endosos*. Nótese que este esquema podrá ser operado y administrado por la CEC-BV de manera exclusiva o compartida. La CAC debe incluir un texto y ciertos datos específicos dispuestos por la Comunicación [\[1933\]](#), además de una referencia a la página de Internet de consulta centralizada mediante su código de visualización.

Finalmente, la Ley N° 27.440 creó la *Factura de Crédito Electrónica MiPyME* (FCE) tipificada en el Título I de dicha ley, que permite a las MiPyME que facturan a empresas grandes *acceder al descuento bursátil de sus facturas electrónicas*, es decir, instrumenta un tipo de factoring bursátil [\[1934\]](#).

En efecto, las FCE se crean con la finalidad de ser negociadas en los Mercados autorizados por la CNV conforme a su reglamentación [\[1935\]](#), y con el mismo tratamiento impositivo correspondiente a los valores negociables con oferta pública, incluyendo su negociación mediante herramientas o sistemas informáticos que faciliten la realización de operaciones de factoraje, cesión, descuento y/o negociación de facturas, las que no serán considerados "Mercados" en los términos del art. 2° de la Ley N° 26.831, ni necesitarán autorización previa y/o para funcionar de la Comisión Nacional de Valores, en tanto solo participen en calidad de compradores, adquirentes, cesionarios o endosatarios las entidades financieras sujetas al régimen de la Ley N° 21.526 así también como los proveedores no financieros de crédito –personas jurídicas que, sin ser entidades financieras realicen - como actividad principal o accesoria- oferta de crédito al público en general, otorgando de manera habitual financiaciones alcanzadas, incluyendo las asociaciones mutuales, las cooperativas y las empresas no financieras emisoras de tarjetas de crédito y/o compra - cualquiera sea su naturaleza jurídica-.

La FCE es un nuevo título ejecutivo y valor no cartular, conforme al art. 1850, CCCN cuando reúne estos requisitos:

- i) se emitan en el marco de un contrato de compraventa de bienes o locación de cosas muebles, servicios u obra;
- ii) Ambas partes contratantes se domicilien en el territorio nacional; y
- iii) se convenga entre las partes un plazo para el pago del precio superior a los quince (15) días corridos contados a partir de la fecha de recepción de la "Factura de Crédito Electrónica MiPyMEs" en el domicilio fiscal electrónico del obligado al pago; (iv) el comprador o locatario, adquiera, almacene, utilice o consuma las cosas, los servicios o la obra para integrarlos, directa o indirectamente, en un proceso de producción, transformación, comercialización o prestación a terceros, sea de manera genérica o específica.

Cuando se hubiera convenido un plazo para el pago del precio *menor* a los 15 días corridos, y vencido el mismo no se hubiera registrado la cancelación o aceptación expresa de la obligación en el "Registro de Facturas de Crédito Electrónicas MiPyMEs", la FCE oportunamente emitida pasará a constituir "título ejecutivo y valor no cartular" desde el vencimiento del plazo de quince (15) días corridos a partir de su recepción en el domicilio fiscal electrónico del obligado al pago, momento en el cual tendrá un nuevo vencimiento el cual será de quince (15) días corridos a los fines de poder ser negociada.

Las notas de débito y crédito que ajusten la operación y por lo tanto a la FCE emitida, deberán generarse dentro del plazo de 15 días corridos desde la recepción de la mencionada factura en el domicilio fiscal electrónico del obligado al pago, hasta la aceptación expresa, lo que ocurra primero.

El comprador o locatario estará obligado a aceptar la FCE salvo casos de:

- (a) daño en las mercaderías, cuando no estuviesen expedidas o entregadas por su cuenta y riesgo;
- (b) vicios, defectos y diferencias en la calidad o en la cantidad, debidamente comprobados;
- (c) divergencias en los plazos o en los precios estipulados;

- (d) no correspondencia con los servicios o la obra efectivamente contratados;
- (e) existencia de vicios formales que causen su inhabilidad, lo que generará la inhabilidad de la FCE tanto como título ejecutivo y valor no cartular, así como documento comercial;
- (f) falta de entrega de la mercadería o prestación del servicio;
- (g) cancelación total de la factura de la FCE. El rechazo de una FCE por las causales previstas en los eventos (a) al (f) debe efectuarse dentro de los diez días corridos de recibida, conforme al Art. 1145, CCCN.

En Enero de 2020, a medio año de su debut, las FCE ya habían desplazado al pagaré bursátil en volumen de operaciones, totalizando \$390 millones mensuales, mientras que el pagaré avalado operó un volumen de \$195, casi cinco veces menos que su máximo volumen operado en Julio de 2019, que ascendió 954 millones de Pesos [\[1936\]](#).

Como puede apreciarse, el Derecho *también* puede innovar. Y es necesario que ello ocurra, por más que la cultura legal no sea tan dinámica como otras culturas, e.g., la de la programación y en general, la *cultura tecnológica*. Estas cuatro muy importantes *innovaciones jurídicas* en materia de instrumentos para la financiación del capital de trabajo nos van acercando, de a poco, al mercado de capitales y sus instituciones, que también han sido fuertemente modificadas y *aggiornadas* por la Ley N° 26.831 de 2012 y por la Ley N° 27.440 de 2018, y también por las modificaciones introducidas al Reglamento General de la Actividad Aseguradora por la Resolución 515/2019 dictada por la Superintendencia de Seguros de la Nación para impulsar el financiamiento PYME y la financiación hipotecaria [\[1937\]](#), así como por algunas normas innovadoras del BCRA en materia de garantías para el financiamiento para la construcción [\[1938\]](#).

5.2.3. *Funcionamiento e instituciones del mercado de*

capitales argentino ^[1939]

El mercado de capitales es el mecanismo a través del cual se produce un intercambio de activos financieros y se determinan sus precios ^[1940]. No requiere un espacio físico y un mercado financiero puede funcionar por medio de computadoras.

Sus funciones son (i) la de poner en contacto a los agentes, sean agentes especializados, o intermediarios; (ii) fijar el precio de los activos, sea en mercados de emisión primaria ^[1941] o de negociación secundaria ^[1942]; (iii) darle liquidez a los activos, ya que mientras más desarrollo tenga un mercado, más fácil es convertir un activo financiero en dinero; (iv) reducir los plazos y los costos de intermediación, aspirando a que las comisiones por operar sean bajas y a que los mercados sean rápidos, en el sentido de que el tiempo que corre entre que se *acuerda* y se *liquida* una operación sea el menor posible. A su vez, mientras más participantes tenga un mercado, menos probabilidades hay de que puedan éstos manipular los precios ^[1943].

Puntualiza Camerini que los mercados monetarios o de dinero, son los mercados en los que se negocian activos *a corto plazo*, normalmente, con vencimientos menores a un año. Está formado por dos grandes bloques: el mercado *interbancario* y el resto de mercados de dinero. Se los clasifica en: (i) mercados de crédito a corto plazo –préstamos, descuentos de facturas comerciales, etc.; y (ii) mercados de títulos valores: se negocian letras del tesoro y títulos emitidos por empresas –cheque y pagarés bursátil, obligaciones negociables de corto plazo– y también emitidos por bancos –depósitos interbancarios, títulos hipotecarios–.

El mercado monetario es un mercado mayorista, ya que sus participantes son grandes instituciones financieras o empresas industriales, que negocian grandes cantidades de recursos de manera muy profesionalizada ^[1944]. Se negocian activos de muy bajo riesgo dada la solvencia de sus emisores, y muy líquidos, con vencimientos cortos y mucha negociación secundaria. El mercado monetario es una parte muy importante del mercado financiero de un país, ya que permite que los fondos líquidos de los sectores superavitarios

lleguen a los sectores deficitarios.

Los mercados de capitales [\[1945\]](#), a su turno, son aquellos en los que se ofrecen y demandan recursos financieros *de largo plazo*, con el fin de potenciar procesos de inversión. Se lo divide en (i) mercado de valores, bursátil, o de bolsa; y (ii) el mercado de crédito a largo plazo. A su vez, el mercado de valores puede dividirse en mercado de renta fija –títulos que pagan un interés fijo– y mercado de renta variable –su rentabilidad depende de la existencia y reparto de beneficios por parte del emisor, i.e. acciones, cuotapartes de fondos comunes de inversión y certificados de participación en fideicomisos financieros– [\[1946\]](#).

A su vez, los mercados pueden estar sujetos a normas y reglamentos de negociación y cotización, como ocurre con una bolsa de valores, en la que intervienen agentes registrados, existen reglas respecto a cómo realizar los intercambios, inscribir los títulos, fijar cotizaciones, etc. O pueden operar *over the counter* (OTC), sin reglamentos ni sistemas pre-determinados para conformar el precio. Estos mercados permiten el intercambio de activos directamente entre agentes o intermediarios, y de acuerdo a las condiciones de precio y cantidad que libremente fijen las partes del modo que prefieran.

Siempre siguiendo a Camerini, afirma que desde 1968 hasta 2012 que se dictó la Ley N° 26.831, en Argentina regía un sistema *de control público* de la oferta pública, en cabeza de CNV, y un sistema de control privado de *cotización, delegado* en las bolsas de comercio si éstas tenían, a su vez, un mercado adherido [\[1947\]](#).

Era un sistema complejo y bien criollo, sin ningún antecedente comparable, ya que los intermediarios que actuaban en el mercado de valores a nivel local, debían adquirir una acción del mercado donde operaban, y quedaban sometidos a la fiscalización *privada* de dicho mercado. Era un sistema de auto-regulación, donde la CNV no tenía facultades para fiscalizar ni sumariar ni sancionar a los agentes y sociedades de bolsa; sólo el mercado en el que éstos operaban podía sancionarlos [\[1948\]](#), y la CNV, a su turno, tenía poder de policía sobre todos los mercados del país, a los que sí podía

sumariar y sancionar.

El sistema descripto fue cambiado en 2012 con la Ley N° 26.831 que eliminó la auto-regulación, y delegó en CNV tanto el control de la *oferta pública* [1949] como el de la *cotización* en mercados autorizados. Las bolsas con mercados adheridos perdieron así la facultad de otorgar cotización a través de sus propias comisiones de títulos –siendo ahora CNV la encargada de ello– y fueron forzadas a integrarse en un nuevo formato de sociedades anónimas [1950].

5.2.3.1. *El rol de la Comisión Nacional de Valores*

Evidentemente, el rol de la CNV en el mercado de capitales es muy trascendente con la nueva Ley N° 26.831. En efecto, la CNV debe (i) regular los títulos valores; (ii) supervisar el sistema operacional; y (iii) tratar las situaciones de crisis del sistema.

Al regular los títulos valores, se ordena el *acceso* al mercado, fijándose los requisitos que deben cumplir las empresas para captar ahorro. Al supervisar el sistema operacional, se supervisa a los intermediarios y a los mercados, así como a los demás agentes involucrados. Finalmente, la CNV debe también resolver las crisis que se presentan, sea de una emisora o sea un intermediario [1951]. Para cumplir sus fines, CNV goza de amplias facultades, reguladas en los arts. 19 y 20 de la Ley N° 26.831, modificada en 2018 por la Ley N° 27.440.

El Art. 19 dispone que CNV tiene las siguientes funciones:

- (a) en forma directa e inmediata, supervisar, regular, inspeccionar, fiscalizar y sancionar a todas las personas humanas y/o jurídicas que, por cualquier causa, motivo o circunstancia, *desarrollen actividades relacionadas con la oferta pública de valores negociables*, otros instrumentos, operaciones y actividades contempladas en la presente ley y en otras normas aplicables, que por su actuación queden bajo su competencia.

El organismo podrá requerir a los mercados y cámaras compensadoras que ejerzan funciones de supervisión, inspección y fiscalización sobre sus miembros participantes. Dicho requerimiento no implicará una delegación de facultades a los mercados y cámaras compensadoras;

(b) llevar el registro, otorgar, suspender y revocar la *autorización de oferta pública de valores negociables* y otros instrumentos y operaciones;

(c) llevar el registro de todos los sujetos autorizados para ofertar y negociar públicamente valores negociables, y establecer las normas a las que deban ajustarse los mismos y quienes actúen por cuenta de ellos;

(d) llevar el registro, otorgar, suspender y revocar la autorización para funcionar de los mercados, cámaras compensadoras, los agentes registrados y las demás personas humanas y/o jurídicas por sus *actividades vinculadas al mercado de capitales*, y a criterio de CNV queden comprendidas bajo su competencia. El registro será público y en él se inscribirán todos los mercados, cámaras compensadoras, agentes y las demás personas humanas y/o jurídicas que por sus actividades vinculadas al mercado de capitales, y a criterio de la CNV queden comprendidas bajo su competencia;

(e) aprobar los estatutos, reglamentos y toda otra normativa de carácter general dictada por los mercados y cámaras compensadoras y revisar sus decisiones, de oficio o a petición de parte, en cuanto se tratare de medidas vinculadas a la actividad regulada que prestan o que pudieren afectar su prestación;

(f) cumplir las funciones delegadas por la Ley N° 22.169 y sus modificaciones respecto de las personas jurídicas alcanzadas por dicha ley en materia de control societario;

(g) dictar las reglamentaciones que deberán cumplir las

personas humanas y/o jurídicas y las entidades autorizadas en los términos del inciso d), desde su inscripción y hasta la baja del registro respectivo;

(h) *dictar las reglamentaciones que se deberán cumplir para la autorización de los valores negociables*, instrumentos y operaciones del mercado de capitales, y hasta su baja del registro, contando con facultades para establecer las disposiciones que fueren necesarias para complementar las que surgen de las diferentes leyes y decretos aplicables a éstos, así como resolver casos no previstos e interpretar las normas allí incluidas dentro del contexto económico imperante, para el desarrollo del mercado de capitales;

(i) *declarar irregulares e ineficaces*, a los efectos administrativos los actos sometidos a su fiscalización cuando sean contrarios a esta ley, a las demás leyes aplicables, a las reglamentaciones dictadas por la CNV, a los estatutos, a las disposiciones dictadas por entidades y aprobadas por el organismo;

(j) promover la defensa de los intereses de los inversores;

(k) establecer normas mínimas de capacitación, acreditación y registro para el personal de los agentes registrados o para personas humanas y/o jurídicas que desempeñen tareas vinculadas con el asesoramiento al público inversor;

(l) determinar los requisitos mínimos a los que deberán ajustarse quienes presten servicios de auditoría a las personas sujetas a su supervisión;

(m) propender al desarrollo y fortalecimiento del mercado de capitales creando o, en su caso, *propiciando la creación de productos que se consideren necesarios a ese fin*;

(n) organizar y administrar archivos y antecedentes relativos a la actividad de la propia CNV o datos obtenidos en el ejercicio de sus funciones para la recuperación de la información relativa a su misión, pudiendo celebrar acuerdos y contratos con

organismos nacionales, internacionales y extranjeros a fin de integrarse en redes informativas de tal carácter, para lo que deberá tenerse en cuenta como condición necesaria y efectiva la reciprocidad conforme las previsiones establecidas en los Art. 25 y 26 de la Ley N° 26.831;

(o) fijar los requerimientos patrimoniales que deberán acreditar las personas humanas y jurídicas sometidas a su fiscalización;

(p) *dictar normas complementarias en materia de prevención de lavado de dinero y de la financiación del terrorismo*, siguiendo la normativa dictada por la Unidad de Información Financiera, organismo autárquico actuante en el ámbito del Ministerio de Finanzas, aplicable al mercado de capitales y fiscalizar su cumplimiento; ello, sin perjuicio del deber de dar a la citada unidad la debida intervención que le compete en materia sancionatoria y de proporcionar a ésta la colaboración exigida por la Ley N° 25.246 y sus modificatorias. La CNV reglamentará la forma en que se difundirán las sanciones que aplique la Unidad de Información Financiera en materia de prevención de lavado de activos y de la financiación del terrorismo, respecto de los sujetos que actúan bajo la órbita de la competencia de dicho organismo;

(q) regular la forma en que se efectivizará la información y fiscalización exigidas en la presente ley, pudiendo requerir a los entes sujetos a su jurisdicción la implementación de aquellos mecanismos que estime convenientes para un control más efectivo de las conductas descriptas en la presente ley;

(r) establecer regímenes de información y requisitos para la oferta pública diferenciados;

(s) determinar las condiciones bajo las cuales los agentes registrados, que revisten el carácter de personas jurídicas, podrán estar habilitados para llevar a cabo más de una actividad bajo competencia de la CNV, previa inclusión de las mismas dentro de su objeto social, a los fines de su inscripción

en los registros respectivos a cargo del organismo;

(t) fiscalizar el cumplimiento objetivo y subjetivo de las normas legales, estatutarias y reglamentarias en lo referente al ámbito de aplicación de la presente ley;

(u) ejercer todas las demás funciones que le otorguen las leyes, decretos y los reglamentos aplicables;

(v) fijar los requisitos de idoneidad, integridad moral, probidad y solvencia que deberán cumplir quienes aspiren a obtener autorización de la CNV para actuar como mercados, cámaras compensadoras y agentes registrados así como los integrantes de sus órganos de administración y fiscalización, según corresponda;

(w) crear nuevas categorías de agentes registrados y modificar las existentes, así como también eliminar las que sean creadas por su propia normativa;

(x) fijar los aranceles máximos que podrán percibir los mercados, cámaras compensadoras, entidades de registro de operaciones de derivados y agentes registrados teniendo en cuenta, entre otros aspectos, la competitividad del mercado de capitales de la región en relación con los aranceles fijados en otros países. Esta facultad se ejercerá en los casos en que -a criterio del organismo- situaciones especiales así lo requieran;

(y) dictar normas tendientes a promover la transparencia e integridad de los mercados de capitales y a evitar situaciones de conflictos de intereses en los mismos; y

(z) evaluar y dictar regulaciones tendientes a mitigar situaciones de riesgo sistémico.

El art. 20, por su parte, dispone que en el marco de la competencia establecida en el art. 19 y teniendo siempre en consideración la protección de los intereses de los accionistas minoritarios y de los tenedores de títulos de deuda, la CNV puede:

- (a) solicitar informes y documentos, realizar investigaciones e inspecciones en las personas humanas y jurídicas sometidas a su fiscalización, citar a declarar, tomar declaración informativa y testimonial, instruir sumarios e imponer sanciones en los términos de la presente ley;
- (b) requerir al juez competente el auxilio de la fuerza pública;
- (c) requerir al juez competente el allanamiento de lugares privados con el fin de obtener los antecedentes e informaciones necesarios para el cumplimiento de sus labores de fiscalización e investigación;
- (d) iniciar acciones judiciales y reclamar judicialmente el cumplimiento de sus decisiones;
- (e) denunciar delitos o constituirse en parte querellante;
- (f) Solicitar todo tipo de información a organismos públicos y a cualquier persona humana o jurídica que considere necesaria para el cumplimiento de sus funciones, quienes estarán obligados a proporcionarlos dentro del término que se les fije bajo apercibimiento de ley. Esta disposición no regirá respecto de la Unidad de Información Financiera.

5.2.3.2. La oferta pública de títulos valores, la contratación bursátil y los intermediarios bursátiles

La Ley N° 26.831 define en su art. 2 a los *valores negociables* como títulos valores emitidos tanto en forma cartular así como a todos aquellos valores incorporados a un registro de anotaciones en cuenta incluyendo, en particular, los valores de crédito o representativos de derechos creditorios, las acciones, las cuotapartes de fondos comunes de inversión, los títulos de deuda o certificados de participación de fideicomisos financieros o de otros vehículos de inversión colectiva y, en general, cualquier valor o contrato de inversión o derechos de crédito homogéneos y fungibles, emitidos o agrupados en serie y negociables en igual forma y con efectos similares a los

títulos valores; que por su configuración y régimen de transmisión sean susceptibles de tráfico generalizado e impersonal en los mercados financieros. Asimismo, quedan comprendidos dentro de este concepto, los contratos de futuros, los contratos de opciones y los contratos de derivados en general que se registren conforme la reglamentación de la CNV, y los cheques de pago diferido, certificados de depósitos de plazo fijo admisibles, facturas de crédito, certificados de depósito y warrants, pagarés, letras de cambio, letras hipotecarias y *todos aquellos títulos susceptibles de negociación secundaria en mercados*.

El mismo art. 2 define a la *oferta pública* como una *invitación* que se hace a personas en general o a sectores o a grupos determinados para realizar cualquier acto jurídico con valores negociables, efectuada por los emisores, por sus tenedores o por organizaciones unipersonales o sociedades dedicadas en forma exclusiva o parcial al comercio de aquéllos, por medio de ofrecimientos personales, publicaciones periodísticas, transmisiones radiotelefónicas, telefónicas o de televisión, proyecciones cinematográficas, colocación de afiches, letreros o carteles, programas, medios electrónicos incluyendo el uso de correo electrónico y redes sociales, circulares y comunicaciones impresas o cualquier otro procedimiento de difusión.

El emisor –i.e, el creador– de valores negociables pretende captar recursos financieros para su actividad específica, ofreciéndolos al público en general por cualquier procedimiento de difusión, *incluyendo la diseminación de información a través de Internet*, y para realizar actos jurídicos sobre valores negociables.

Para poder hacer tal tipo de invitación, debe *previamente* pedir autorización a CNV, bajo apercibimiento de que el ofrecimiento encuadre como *oferta pública irregular*. Señala Camerini que no necesitan pedir autorización previa los títulos valores emitidos por la Nación, las provincias, las municipalidades, los entes autárquicos y las empresas del Estado ^[1952].

En lo atinente a la contratación bursátil, el art. 1429, CCCN dispone que los contratos celebrados en una bolsa o mercado de comercio, de valores o de productos, en tanto éstos sean autorizados y operen bajo contralor estatal, se rigen por las normas dictadas por sus autoridades y aprobadas por el organismo de control. Estas normas pueden prever la liquidación del contrato

por diferencia; regular las operaciones y contratos derivados; fijar garantías, márgenes y otras seguridades; establecer la determinación diaria o periódica de las posiciones de las partes y su liquidación ante eventos como el concurso, la quiebra o la muerte de una de ellas, la compensación y el establecimiento de un saldo neto de las operaciones entre las mismas partes y los demás aspectos necesarios para su operatividad.

En relación a los intermediarios bursátiles, sostiene Camerini que durante mucho tiempo, el agente de bolsa fue considerado un simple corredor que asesoraba a las partes y las acercaba, pero no podía exigir el cumplimiento del contrato, sino sólo cobrar comisiones.

Con el tiempo, el simple corredor se convirtió en comisionista, actuando por cuenta propia o ajena, pudiendo exigir el cumplimiento del contrato. En la actualidad, hay agentes que sólo actúan en nombre propio pero por cuenta ajena, *brokers o comisionistas*, y que cobran una comisión por operación; y hay también agentes que actúan por nombre y cuenta propia, cuya ganancia consiste en la diferencia de precio entre la compra y la venta de un título valor [\[1953\]](#).

La Ley N° 26.831 facultó a la CNV a crear registros públicos para la actividad de negociación, colocación, distribución, corretaje, liquidación y compensación, custodia y depósito colectivo de títulos valores, etc, y creó también nuevas denominaciones para tales actividades [\[1954\]](#)

Así, la intermediación bursátil desde el año 2012 se centraliza en CNV, quien ha tipificado a los agentes de negociación (AN) [\[1955\]](#), agentes de liquidación y compensación (ALyC) [\[1956\]](#), y agentes de depósito colectivo (Caja de Valores) [\[1957\]](#).

5.2.3.3. *Algunas innovaciones jurídicas en el mercado de capitales argentino*

En los últimos años, han tenido lugar algunas importantes innovaciones jurídicas a nivel de mercado de capitales. Se resaltarán a continuación las más

importantes.

5.2.3.3.1. Regulación de los contratos derivados

La Ley N° 27.440, de *Financiamiento productivo*, reguló en el Título VIII, arts. 188 a 194, a los instrumentos derivados.

Se define a los derivados como contratos (i) sujetos a la ley y jurisdicción argentina o extranjera y celebrados bajo acuerdos marcos, individuales y/o bajo los términos y condiciones establecidos por el mercado en el que se concerten; (ii) en los cuales sus términos y condiciones, incluyendo precio, cantidad, garantías y plazo, *derivan o dependen de un activo o producto subyacente*, los que pueden consistir en activos financieros, tasas de interés, índices financieros, valores negociables y/o activos no financieros (cereales, minerales, alimentos, inmobiliarios); (iii) que se pueden celebrar y/o negociar en mercados autorizados por la CNV o fuera de los mismos (OTC); y que (iv) si se negocian en mercados autorizados por CNV, les son aplicables ciertos requerimientos de márgenes y garantías: éstos son *otros* contratos bursátiles por los cuales las contrapartes en cada derivado o terceros acuerdan la entrega de valores negociables, activos financieros, dinero, etc. *con la finalidad de asegurar el cumplimiento* de cualquier clase de obligaciones de pago y entrega bajo los derivados.

La importancia económica de los contratos derivados deriva, valga la redundancia, de la posibilidad que ofrecen de alocar de manera eficiente los riesgos financieros.

Así, la transferencia de riesgos a través de contratos –esta es la esencia de un derivado – es muy vieja (p.e., seguros), pero su conveniencia fue puesta en duda con la crisis hipotecaria de 2007-11 por los abusos en su utilización [\[1958\]](#).

Los derivados actuales son la *última innovación* de las Finanzas Corporativas, pero son odiados por muchos, y amados por otros que necesitan cubrirse de distintos riesgos, transfiriéndolos a otras partes dispuestos a correrlos.

Muchos creemos que pueden ser *socialmente eficientes* cuando son bien utilizados ^[1959]. Luego de la crisis financiera de 2007-11, el *Consenso Transatlántico* ^[1960] sobre los derivados sostiene: (1) que los contratos OTC estandarizados deben registrarse (*clearing houses*); (2) debe centralizarse la información para saber cuáles son, dónde están y quién soporta los riesgos; y (3) si un derivado es muy *taylor-made* como para registrarse, debe fortalecerse el riesgo de contraparte.

En cuanto a las especies de derivados, existen derivados cobertura, y también derivados especulativos. En los de cobertura, por ejemplo, una empresa productora de aceite de soja que demanda el grano de la oleaginosa como insumo principal para la elaboración de ese producto, ante expectativas *alcistas* en el precio del grano, puede celebrar un contrato *forward* con su proveedor (el productor agrícola) para cubrirse de la posible volatilidad.

En los contratos derivados de especulación, en cambio, la empresa no busca cubrir o minimizar un riesgo sino que, al contrario, usa derivados para obtener un beneficio derivado del *arbitraje* de un producto por la diferencia entre los precios acordados entre una posición (comprador) y otra (vendedor). Éstos son normalmente contratos OTC, pero los hay también en mercados regulados (ej. opciones).

Los derivados más conocidos y usados son los *forwards*, un contrato para comprar o vender un determinado activo en un momento futuro y a un precio futuro especificado, que se negocia OTC *con riesgo de contraparte* entre entidades financieras o entre éstas y sus clientes.

En un *forward*, una parte asume posición *long* (compradora) por la cual acuerda comprar el activo subyacente y la otra parte asume posición *short* (vendedora). Los subyacentes son commodities, divisas, tasa de interés y acciones. El *forward* más negociado es el de tasa de interés (*forward rate agreements* –FRAs–), seguidos por los de monedas, commodities y acciones.

Los contratos de *futuros*, a su turno, son aquéllos celebrados entre dos partes, por el que se comprometen a intercambiar un activo (activo subyacente) que puede ser físico o financiero, a un precio determinado y en una fecha futura preestablecida. Son usados como respuesta *financiera* ante la

aparición de una volatilidad excesiva en los precios de materias primas/tipos de interés/tipos de cambio, etc. Son instrumentos de gestión del riesgo de fluctuación y *se negocian en un mercado organizado sin riesgo de contraparte.*

Un ejemplo es el contrato tranzado en ROFEX^[1961], futuro Soja Chicago sobre 5 toneladas.

Las opciones, por su parte, son un contrato en el cual una de las partes, llamada titular, mediante el pago de una suma de dinero, llamada prima, *adquiere el derecho pero no la obligación de comprar o vender* a otra parte, llamada lanzador, un determinado bien a un precio, el “precio de ejercicio”, a una fecha o plazo futuro determinada, fecha de ejercicio. La opción de compra se denomina *call*, y de venta *put*. Según el momento en que puede ejercerse la opción, se la llama Europea cuando sólo puede ejercerse en una fecha determinada, o Americana cuando puede ejercerse en cualquier momento. Como los futuros, se negocian normalmente en mercados autorizados sin riesgo de contraparte.

Otros derivados menos frecuentes son los *swaps*^[1962], en donde las partes se comprometan a *intercambiar flujos de fondos periódicos*, denominados en una misma o distintas monedas, tomando en consideración para ello el valor de un bien o de un índice subyacente.

Vía swap una empresa podría, por ejemplo, intercambiar/convertir una tasa fija por una variable, lo que le permitiría disminuir su costo de fondeo maximizando los diferenciales de tasas y su capacidad de crédito. Es una operatoria con riesgo de contraparte y totalmente OTC.

Un ejemplo es el siguiente: un banco que otorga préstamos (que constituye un activo) a un empresa automotriz a una tasa variable BADLAR Privada más un nominal de 3, por un período de 2 años, con pagos de interés mensuales; y, por otro lado, un depositante del banco suscribe un plazo fijo con interés fijo del 10% (que constituye un pasivo), cobrando un interés mensual. Dado que el banco tiene sus activos (préstamos) a tasa variable, y sus pasivos (depósitos) a tasa fija, le puede convenir celebrar un *swap* con alguna contraparte para intercambiar/convertir tasa variable por tasa fija para cumplir con el plazo fijo: así, el banco se comprometerá a pagar al final de cada período de intereses la tasa Badlar Privada +3, a cambio de que la contraparte pague al

vencimiento de cada período de tres meses la tasa fija del 10%. Este tipo de operación se liquida por compensación: calculando la diferencia entre la tasa fija y la variable, y si la tasa fija es mayor que la variable, el pagador de tasa fija (la contraparte) pagará al banco la diferencia y viceversa.

Finalmente, existe también un derivado muy particular, sobre el cual se han cargado las tintas en la última crisis financiera de 2007/11, llamado *credit default swap* -CDS [\[1963\]](#).

Los CDS funcionan *mutatis mutandis* como el seguro de un auto [\[1964\]](#): el comprador realiza una serie de pagos en el tiempo (primas) y el vendedor asume el compromiso de cubrir parte o el total del crédito asegurado, en caso de un "siniestro" (i.e., que el préstamo no fuese cancelado al vencimiento).

Es un contrato muy sofisticado y típicamente OTC con (gran) riesgo de contraparte y se utiliza como seguro de *default* de bonos soberanos, pero también se los utiliza para asegurar defaults privados en securitizaciones.

Es un activo financiero, no negociado en un mercado secundario oficial, mediante el cual el comprador del CDS, a cambio del pago de una prima periódica recibe una indemnización del vendedor del CDS en caso de que un tercero (el emisor de los títulos de deuda) entre en concurso de acreedores o efectúe una quita o espera [\[1965\]](#).

El activo subyacente es valor nominal del préstamo impago. En este sentido, puede ser conceptualizado como un contrato entre dos partes en el que una de ellas *compra protección* sobre el riesgo de default de una cierta cantidad (nocial) de bonos o deuda, de una determinada compañía, durante un plazo especificado, y la otra parte vende esta protección. El comprador paga una prima periódica, denominada "*spread*", a cambio del cual, en caso de que se produzca un *default*, el vendedor compensará al comprador por las pérdidas en esos bonos y el *spread* se dejará de pagar.

Un ejemplo puede servir para terminar de entender la operatoria: si un banco A financia a un deudor B, contrata un *Swap* para cubrirse ante el default de B. El banco A compra un swap al inversor C por el cuál le paga una prima periódica y si B incumple, el inversor C deberá pagarle al banco A la

deuda incumplida por B a su valor par; luego el inversor C se convertirá en el acreedor de B, por lo que la pérdida de C será equivalente a la diferencia entre el valor par de la obligación y el valor de recupero de la deuda.

Muy vinculado a los CDS, debe tenerse presente que en el segmento minorista de seguros, la protección contra el riesgo de crédito financiero puro vía seguros estuvo prohibida en Argentina desde 1973 (Ley N° 20.091 de entidades de seguros) hasta el dictado de la Ley de Financiamiento Productivo en 2018, que modificó el Art. 24 de la Ley N° 20.091 y ahora permite a las aseguradoras ofrecer pólizas seguros de crédito financiero puro sólo cuando se trata de financiación hipotecaria (securitización hipotecaria), siempre y cuando no implique un encarecimiento para los tomadores de dichos créditos, y conforme se reglamente la operatoria por la Superintendencia de Seguros de la Nación.

La posibilidad de poder asegurar en alguna medida el impago hipotecario por parte del deudor (ej: pago de 6 cuotas por pérdida temporal de trabajo), produce una mejora relativa de riesgo de la cartera securitizable, y por ende una baja relativa de tasas de fondeo del originante, pero ante un evento de riesgo sistémico (ej: default hipotecario *subprime* de 2007-11), hasta la aseguradora más grande del mundo cayó por culpa de los CDS suscriptos: [AIG \[1966\]](#) .

Un estudio sobre el Mercado Argentino de Derivados del año 2018 [\[1967\]](#) señalaba que el volumen de dinero pasó de \$ 77 millones en 2008 a \$ 415 millones a Diciembre de 2017, lo que no parece mucho si se lo compara con el tamaño que la industria del seguro tenía en Argentina en 2017: \$ 29 mil millones de Pesos.

El señalado estudio indicaba que de las 77 entidades financieras bajo supervisión del BCRA, 57 informaron alguna operación con derivados. En cuanto a instrumentos, crecen más los futuros (tranzados en mercados autorizados sin riesgo de contraparte) que los *forwards* (tranzados *OTC*, *taylor-made* y con riesgo de contraparte). La cantidad de entidades que operan futuros pasó de 15 en 2008 a 27 en 2017. Del volumen total operado en 2017, aproximadamente el 45% corresponde a futuros, un contrato estandarizado, sin riesgo de contraparte, muy líquido, con un plazo promedio

5 meses, negociado principalmente en ROFEX (97%) y MAE (3%), con el 98% del activo subyacente siendo moneda extranjera.

Un 19% de dicho volumen opera en *forwards* de tipo de cambio a 5 meses. El 4% operaba en swaps a 3 años para cobertura de tasas (variable a fija) y a fines de 2017 venían creciendo los futuros y opciones de trigo y maíz (6% interanual). A su vez, los pases bancarios (REPO) ^[1968] son los más usados por los bancos, 43 de las 77 entidades los utilizaron en 2017.

Luego de esta muy somera introducción a los derivados, se avanzará en su regulación.

En este sentido, el Título VIII de la Ley N° 27.440 se aplica a tres tipos de derivados: (1) Derivados celebrados en el ámbito de mercados autorizados por CNV cuando la liquidación de las operaciones *está a cargo de una cámara compensadora (sin riesgo de contraparte)*; (2) Derivados celebrados en el ámbito de mercados autorizados por CNV *sin cámara compensadora (con riesgo de contraparte: MAE sin garantía / SENEBI sin garantía)*; y(3) los derivados OTC puros: derivados celebrados entre partes nacionales o extranjeras, por fuera del ámbito de mercados autorizados por CNV, pero que *deben registrarse en CNV para tener efectos frente a terceros y fecha cierta*.

Varias veces ya ha salido el término “riesgo de contraparte”. ¿Qué es el riesgo de contraparte? Es su *default*, es decir el incumplimiento basado en su concurso, su quiebra o liquidación. Este riesgo de contraparte no existe dentro de mercados autorizados por CNV, ya que justamente se utilizan otros contratos, los de *márgenes y garantías* con reposición diaria: el mercado siempre pagará, incluso ante el incumplimiento de la contraparte por concurso/quiebra/liquidación.

En cambio, en operaciones con derivados OTC, aún registradas en CNV, el riesgo de contraparte es importante ya que *ningún tercero garantiza el cumplimiento*. Por ello se pactan garantías contractuales auto-liquidables para el evento de *default*, las que sólo son oponibles a terceros si el contrato se registra (pagando consecuentes tasas de registro). Evidentemente, aquí es donde más valor pueden aportar los *Smart Contracts*, y es a dónde más se los utiliza, por cierto.

La Ley de Financiamiento Productivo se propuso con gran tino impulsar el uso de los derivados disminuyendo el riesgo de contraparte, *haciendo prevalecer lo pactado en el contrato derivado celebrado por las partes para el caso de default*, incluso por sobre las normas generales que aplican a todos los contratos en nuestro régimen jurídico.

Así, si un derivado se registra en la CNV: (1) no se aplican algunas normas generales de la Ley de Concursos y Quiebras N° 24.522, (2) no se aplican algunas normas específicas del régimen de liquidación de aseguradoras (Ley N° 20.091); (3) No se aplican algunas normas específicas de liquidación de entidades financieras por el BCRA (Ley N° 21.526) ni del art. 49 de la Carta Orgánica BCRA (Ley N° 24.144); y (4) no se aplican algunas normas generales del CCCN.

Este pequeño *introito* al mundo de los derivados sobre dinero *fiduciario* es relevante, ya que el mercado de derivados sobre *criptoactivos* está creciendo mucho en los mercados más adelantados, tal como ilustra el caso de Japón comentado *supra* en § 3.4.6.1.5 o al comentar el caso de Bakkt en § 4.5.11. Es conveniente que el desarrollo de derivados sobre criptoactivos se amplíe, por cuanto es una forma eficiente de reducir o cubrir la volatilidad del criptoactivo subyacente.

5.2.3.3.2. *Desmaterialización de títulos valores con oferta pública*

Argentina ha sido pionera en aprobar algunas estructuras *innovadoras*, como lo es la securitización de activos digitales.

Básicamente, se ha permitido securitizar préstamos personales originados 100% *on line*, donde el originador identifica al solicitante del préstamo, toda la documentación de la operación es digital, incluyendo la información sobre la morosidad de los créditos securitizados; se le reconoce validez al contrato de préstamo contenido en soporte electrónico *u en otra tecnología similar*, aclarándose que estos préstamos no tienen una acción ejecutiva para el cobro, pero conservan la acción ordinaria ante la falta de pago.

Para securitizar estos préstamos digitales, se recurre al fideicomiso financiero, exigiendo CNV:

- i) un legajo por cada solicitante, y cesión del préstamo al fiduciario para su custodia;
- ii) un proceso de revisión especial del activo fideicomitido digital, a cargo de un Agente de Control y Revisión;
- iii) un registro y backup de la trazabilidad de la navegación que originó el préstamo digital;
- iv) un informe que certifique los procesos de originación, que de cuenta de la inalterabilidad de los datos, la confiabilidad de los soportes, y de la autenticidad de los mensajes entre el originante y el solicitante;
- v) una serie de declaraciones juradas del fiduciante y del fiduciario sobre los procesos de originación y el funcionamiento de los sistemas informáticos, y
- vi) sistemas de identificación fehaciente de la identidad del deudor del préstamo digital securitizado. Los primeros casos fueron MONI Mobile I [\[1969\]](#) y Mercado Crédito I [\[1970\]](#).

Otra importante innovación han sido las ON Simple, que permite que toda la documentación relativa al título a emitir se presente por vía digital a CNV, mediante la utilización de formularios predeterminados.

Finalmente, otra importante innovación ha tenido lugar en la industria de los Fondos Comunes de Inversión. Así, se ha aceptado la colocación de cuotapartes a través de una plataforma digital, que facilita el proceso de inversión en fondos autorizados por CNV. Se utiliza una billetera virtual linkeada a una cuenta corriente del inversor e interviene un Agente de Colocación y Distribución Integral, que suscribe y rescata a nombre propio pero por cuenta de terceros las cuotapartes digitales que se emiten.

Mercado Libre [\[1971\]](#) fue el primer jugador en utilizar esta figura, para ofrecer a sus clientes que abran una cuenta comitente en Banco Industrial – que actúa como ACyDI–, y ofreciendo que los fondos depositados puedan ser invertidos en Mercado Fondo, que es un fondo de renta fija, a través de la

billetera digital de Mercado Pago.

5.2.3.3.3. *Hacia los bonos verdes on-chain: los G-ABS* [\[1972\]](#).

Finalmente, quiero hacer mención a una innovación que se está gestando en el mundo, pero que aún no ha sido testada en Argentina, y sobre la cual tengo especial interés en impulsar. Me refiero un tipo particular de security token que, en mi opinión, demanda inmediatos cambios regulatorios para acelerar su adopción y utilización masiva en el ámbito de las *Finanzas Sustentables*, para poder impulsar la agenda de los Objetivos de Desarrollo Sostenible (“ODS”) [\[1973\]](#).

Así, se propone analizar las nuevas posibilidades que ofrecen los *blockchain-based green bonds*, un tipo de STO caracterizado por la aplicación específica de los fondos recaudados, y por su alineación a los ODS, que constituyen parte del objeto de estudio de las *Finanzas Climáticas*.

5.2.3.3.3.1. *Acelerar las Finanzas Climáticas*

Las Finanzas Climáticas, Verdes o Sustentables tienen como objetivo estructurar mecanismos de financiación para proyectos de *mitigación, adaptación y resiliencia* al cambio climático y que ayuden al cumplimiento de los ODS. Desde esta nueva mirada, comienzan a pensarse y a diseñarse nuevos instrumentos financieros que incluyen un triple criterio de impacto: medioambiental, social y de gobierno corporativo, y bajo cuyo paraguas se incluyen actividades como fondos sustentables, bonos verdes, inversión de impacto, microfinanzas, y créditos para proyectos sustentables [\[1974\]](#). Comienza a verse un flujo creciente de capitales comprometidos con iniciativas como los Principios para la Inversión Responsable [\[1975\]](#) y la Declaración Mundial de los Inversores sobre el Cambio Climático [\[1976\]](#). En efecto, durante 2018, las Finanzas Sustentables captaron inversiones por 167.2 Billones de Dólares, representando el 2% del total de fondos captados a través

de bonos ^[1977], una cifra que impresiona pero que es aún *insuficiente y marginal*.

Como una nueva sub-disciplina del *Corporate Finance*, el auge de las Finanzas Climáticas puede vincularse a dos fechas relevantes: el 25 de Septiembre y el 12 de Diciembre de 2015, fechas en las que se suscriben los Objetivos de Desarrollo Sostenible y el Acuerdo Climático de París, respectivamente.

Desde tales hitos, la comunidad de inversores del mundo desarrollado comienza a acelerar el “*enverdecimiento*” de sus carteras de inversión, generando una oferta de miles de millones de Dólares en busca de este escaso tipo de proyectos. Como contracara de este enfoque pro-activo de *Smart & Green Money* buscando globalmente proyectos “*verdes*”, también comienzan a avistarse enfoques reactivos, impulsados por reguladores e inversores cada vez más preocupados por el impacto social y medioambiental de sus inversiones. El reciente caso Exxon Mobil ^[1978] sin dudas será el primero de muchos, muchos otros, en esta dirección.

En tal contexto, la Sustainable Digital Finance Alliance (SDFA) en colaboración con el HSBC Centre of Sustainable Finance promueven la incorporación de tecnología para facilitar y potenciar los flujos de financiamiento para proyectos alineados con los ODS mediante la emisión de bonos verdes ^[1979].

En línea con la SDFA, se considera necesario promover el debate sobre Finanzas Sustentables en la República Argentina, bajo la firme convicción de que *el tiempo corre en contra de nuestra especie*, y deben planificarse y tomarse drásticas decisiones en los próximos años, muchas de ellas por parte de empresas que están evaluando cómo financiar proyectos.

5.2.3.3.2. Los Valores Negociables SVS

Evidentemente, la iniciativa privada *per se* no puede ni debe cargar con todo el peso de mitigar el cambio climático: los riesgos deben repartirse con el sector público, y se requieren grandes esfuerzos regulatorios desde el sector

público para incentivar fuertemente los flujos de capital hacia proyectos alineados con los ODS.

En este sentido, se advierte que las Normas de la Comisión Nacional de Valores (T.O. 2013) sólo referencian indirectamente a las Políticas de Sustentabilidad [\[1980\]](#), lo que ha motivado que se emitan recientemente unos *Lineamientos para la Emisión de Bonos Verdes, Sociales y Sustentables*, y que se modifiquen ciertos aspectos de las Normas de CNV mediante la Resolución General 788/2019 [\[1981\]](#).

Estos Lineamientos dan al mercado una guía de buenas prácticas y parámetros para la emisión de valores negociables sociales, verdes y/o sustentables (“Valores Negociables SVS”), y difunden los estándares internacionales y pautas para evaluar los activos elegibles, dando pautas a los mercados que pretendan crear etiquetas, paneles o segmentos diferenciados para estos productos.

Analizando los Principios de los Bonos Verdes (Green Bond Principles) [\[1982\]](#) y Bonos Sociales (Social Bond Principles) [\[1983\]](#) emitidos por la International Capital Market Association (ICMA) y el Estándar Internacional para los Bonos Climáticos gestionado por la Climate Bonds Initiative (CBI) [\[1984\]](#), los Lineamientos afirman que cada una de las etiquetas de los Valores Negociables SVS se define en función de los beneficios generados por los proyectos o actividades a ser financiados.

Así, los valores negociables “*verdes*” se centran en proyectos o actividades con beneficios ambientales, los valores negociables “*sociales*” en proyectos o actividades con beneficios sociales, y los valores negociables “*sustentables*” persiguen una combinación de ambos. Afirma CNV que los Valores Negociables SVS son estructurados de manera similar a cualquier valor negociable tradicional, pero la diferencia radica en el *uso que se le dará al financiamiento obtenido*, el cual debe ser exclusivamente asignado a actividades o proyectos que califiquen como sociales, verdes o sustentables, lo que deberá encontrarse detallado en el respectivo prospecto de emisión.

CNV señala que la normativa argentina permite estructurar emisiones SVS

con formato de obligación negociable, con o sin garantía flotante, especial o común, obligación negociable PYME, obligación negociable simple con garantía por una entidad listada en CNV, bonos estructurados a través de una *special purpose vehicle*, fondos comunes de inversión y fideicomisos financieros.

En la visión de CNV, los Valores Negociables SVS promueven una mayor transparencia ya que requieren “*demostrar que el financiamiento recaudado fue efectivamente utilizado para financiar proyectos con beneficios ambientales o sociales*”^[1985], y afirma que existe evidencia de beneficios de tasas para emisores, debido a la fuerte demanda y oferta limitada de estos productos, siendo habitual la sobresuscripción.

En relación al carácter sustentable del proyecto y al destino de los fondos, para evitar el *green washing*^[1986], CNV señala que preponderan las revisiones externas que refuerzan la credibilidad de la etiqueta, mediante una segunda opinión, verificación, certificación o rating. En este sentido, respecto a la administración y trazabilidad de los fondos, CNV afirma que estos activos “**deben ser asignados a cuentas específicas, u otros **mecanismos confiables que garanticen la trazabilidad y la transparencia en el uso de los fondos****”^[1987], afirmando CNV que “los ingresos netos se pueden acreditar a una subcuenta, o **rastrearse de otra manera apropiada**”^[1988], informando sobre los recursos invertidos y los recursos no asignados, en éste caso indicando las inversiones temporales. (el resaltado me pertenece).

Finalmente, indica CNV que el impacto de estos proyectos se informa anualmente mediante reportes, validados por un revisor externo independiente, donde se discrimina el destino de la financiación o de la refinanciación emitida, y el impacto medido mediante indicadores de desempeño cualitativos y cuantitativos. CNV remite en este aspecto a las recomendaciones sobre el reporte de impacto ambiental y social emitidas por la ICMA^[1989].

5.2.3.3.3.3. Estímulo Fiscal

Hasta aquí, los primeros pasos de nuestro regulador bursátil permiten avistar un tenue viraje regulatorio, más amigable hacia el fenómeno de las Finanzas Climáticas, pero no se está viendo un claro estímulo fiscal en la misma dirección, cuestión que es también necesaria y esencial.

En efecto, el necesario y urgente cambio de paradigma hacia la Sustentabilidad requiere fuertes niveles de inversión pública, que se manifestará como esquemas tributarios específicos que estimulen actividades que reduzcan la emisión de Gases de Efecto Invernadero (“GEI”), la generación de energía a través de energías renovables, el aumento de la eficiencia energética, o nuevas formas de producción que sean bajas en consumo y emisión de carbón.

Por caso, en California existe un *tax shield* equivalente al 30% de toda inversión dirigida a las energías renovables; en Alemania existen tasas de interés subsidiadas y préstamos blandos para proyectos de eficiencia energética; en Francia existen estímulos de amortización acelerada para equipamiento utilizado en la generación de energía renovable; Rusia combina amortizaciones aceleradas con diferimientos impositivos para adquirir bienes eficientes en el uso de energía; y China directamente introdujo exenciones fiscales en el impuesto a las sociedades para proyectos de inversión en energías renovables [\[1990\]](#).

En Argentina, debe resaltarse como un primer paso muy importante el Régimen de Fomento de Energías Renovables impulsado por las Leyes N° 26.190 y 27.191 y su reglamentación. Los beneficios fiscales de este régimen incluyen la devolución anticipada del IVA correspondiente a los bienes nuevos incluidos en el proyecto, y la posibilidad de su amortización acelerada en el Impuesto a las Ganancias. Se admite también la compensación de quebrantos con ganancias, la cual podrá realizarse únicamente con pérdidas originadas por el desarrollo de la actividad promovida por el Régimen de Fomento de Energías Renovables. Asimismo, se prevé que los bienes afectados al proyecto no integrarían la base de imposición del Impuesto a la Ganancia Mínima Presunta (derogado a partir del 1/01/19).

Finalmente, reconociendo el carácter típico de *Project Finance* de estos proyectos, se admite la deducción de la carga financiera del pasivo financiero,

pudiendo deducirse de las pérdidas de la sociedad los intereses y las diferencias de cambio originados por la financiación del proyecto, y se los exime del impuesto sobre la distribución de dividendos o utilidades en la medida que esos dividendos o utilidades sean reinvertidos en un nuevo proyecto de infraestructura en el país.

5.2.3.3.3.4. *Green Blocks: kickstarting the blockchain-based green bonds Industry*

Tal como pregona CNV, el éxito en la utilización masiva de los Valores Negociables SVS depende, por un lado, de (i) evitar el *green washing*, y, por otro, de que (ii) los Valores Negociables SVS garanticen al inversor que el financiamiento recaudado fue efectivamente utilizado para financiar proyectos con reales beneficios ambientales o sociales, beneficios éstos que deben ser medibles, trazables y comunicados. Actualmente, esta medición de impacto *depende de terceros* que auditan el ciclo de vida de los activos verdes, lo que implica costos de estructura y operación que pueden representar una barrera a la entrada al mercado para emisores pequeños y medianos.

Ahora bien, para cumplir ambos objetivos, la tecnología *blockchain* está llamada a jugar un papel central, en combinación con otras tecnologías: Internet of Things (IoT) y la Inteligencia Artificial (AI), mix tecnológico que permitirá emitir reportes automáticos que aumentan la trazabilidad de los fondos recaudados con bonos verdes, informando en tiempo real el impacto generado por el proyecto a través de distintas métricas. Sumado a estos beneficios para el inversor, la emisión de bonos en *blockchain* elimina intermediarios, y permite reducir aproximadamente 10 veces el costo de emisión y estructuración de bonos verdes, lo que permite que más emisores y proyectos más pequeños accedan a un financiamiento masivo [\[1991\]](#).

En este sentido, la S DFA sostiene que la utilización de *blockchain* permite digitalizar la confianza usando algoritmos matemáticos y criptografía para validar transacciones, reduciendo costos de intermediarios y disminuyendo el tamaño de los tickets de inversión, lo que posibilita ampliar la base de inversores. Al combinarse con IoT y AI, *blockchain* permite capturar datos a través de sensores instalados en un activo verde, y exponerlos a los inversores

en tiempo real a través de su billetera digital, como un nuevo modo de “Prueba de Impacto” de la inversión [\[1992\]](#).

Señala la S DFA que la utilización de *blockchain* en la emisión de bonos verdes tendrá impacto en tres áreas críticas: (i) estructuración, emisión y distribución [\[1993\]](#); (ii) transferencia de propiedad, pagos y liquidaciones [\[1994\]](#); y (iii) reportes sobre utilización de los fondos y prueba de impacto. En las dos primeras áreas, ya existen antecedentes que serán analizados seguidamente.

5.2.3.3.3.5. *Bond-i: el Canguro disruptivo*

El Banco Mundial (BM), junto con el Commonwealth Bank of Australia (CBA), fueron los *early adopters* de los *blockchain-based-bonds* en Agosto de 2018, en el proyecto que denominaron “Bond-i” [\[1995\]](#). Se trata del *leading case* en aplicar la tecnología *blockchain* a todo el ciclo de vida de un bono, desde su estructuración, emisión, distribución, transferencia, gestión de tenencias de los inversores y negociación secundaria.

Este bono a dos años recaudó 110 Millones de Dólares Australianos en su primera serie, ofreciendo un cupón de 2.20% anual, pagadero semestralmente, por período vencido [\[1996\]](#). En Agosto de 2019, se emitió una segunda serie por 50 Millones de Dólares Australianos [\[1997\]](#). La plataforma Bond-i corre en una versión privada de la *blockchain* Ethereum, y mediante *Smart Contracts* automatizó el proceso de subasta electrónica y book building, entregando informes en tiempo real a los inversores de acuerdo a los permisos de acceso a una red privada pero permissionada, permitiendo auditar todo el proceso de transacciones registradas en la cadena de bloques de manera inmutable. La arquitectura de la *blockchain* fue auditada por Microsoft.

Para poder acceder a la plataforma Bond-i, los participantes e inversores fueron previamente autenticados por BM y CBA, realizándose el proceso de Know Your Customer off-chain. La plataforma Bond-i permite el registro de

las tenencias sin necesidad de contratar agentes de custodia, un rápido procesamiento para los inversores, sin necesidad de reconciliar datos, otorga visibilidad total de las transacciones para el BM, y emite reportes inmediatos para el regulador bursátil, quien tiene un nodo en la *blockchain* con facultad de observar las transacciones [\[1998\]](#).

5.2.3.3.3.6. *El primer bono verde emitido en blockchain*

En febrero de 2019, el banco español BBVA emitió el primer bono verde en *blockchain*, por un valor de 35 Millones de Euros, utilizando una plataforma propia que permite al cliente estructurar el instrumento de manera directa [\[1999\]](#), con un enfoque de auto-servicio y un proceso totalmente digital, desde la negociación hasta la emisión. El carácter “verde” del bono fue certificado por una ‘Second Party Opinion’ emitida por [DNV GL](#), entidad de certificación líder a nivel mundial [\[2000\]](#).

Se trata de un bono a 6 años, que busca recaudar fondos para financiar proyectos verdes en el marco de la política de sustentabilidad de BBVA. La emisión fue suscrita íntegramente por la aseguradora Mapfre, y se trata de la séptima emisión de bonos utilizando *blockchain* que lleva adelante BBVA [\[2001\]](#).

BBVA utilizó una versión de HyperLedger Fabric, una *blockchain* privada permitida, que otorga permisos de acceso sólo a contrapartes autorizadas -e.g., inversores-. El registro de transacciones se hace en la *blockchain* pública Ethereum Testnet para dar visibilidad total a cualquier observador. Vale resaltar que BBVA ofrece a sus clientes la opción de tener un nodo de la *blockchain*.

5.2.3.3.3.7. *On-chain payments: StableCoins y Central Bank Digital Currencies*

Las ganancias de eficiencia que se obtienen por migrar *on-chain* el proceso tradicional *off-chain* de negociación, estructuración, emisión, distribución,

transferencia, custodia y negociación secundaria son evidentes y están fuera de discusión. Ésta será una tendencia creciente que disruptará varios segmentos en el mercado de servicios financieros que, hasta el presente, han mantenido ciertos privilegios legales de índole regulatoria que representan, en términos Antitrust, altas barreras a la entrada a nuevos jugadores y, en términos del Análisis Económico del Derecho, mayores costos de transacción para los agentes económicos.

Ahora bien, el verdadero desafío que las Finanzas Sustentables demandan va más allá, e implica migrar *on-chain* los pagos y liquidaciones de bonos verdes mediante monedas estables o avaladas por Bancos Centrales. Tanto en el caso del bono “Canguro” como del bono verde de BBVA, los pagos y liquidaciones se siguen haciendo *off-chain*, es decir, no están automatizados vía *Smart Contracts*.

La creación de StableCoins ya desarrolladas en § 3.4.6, 3.4.4.1, 3.4.1.2 y 3.4.2.2.3 implica hablar de un activo digital en *blockchain* vinculado a alguna o algunas monedas *fiat* nacionales, se las denomina “*Cash On Ledger*” en lugar de “Coins”, para desmarcarse del riesgo asociado a los cripto-activos en general.

Los bancos están comenzando a emitir sus propias StableCoins, como por ejemplo la moneda de JP Morgan: JPMCoin, creada en Febrero de 2019 [\[2002\]](#) y que tiene una paridad 1 a 1 con el Dólar Norteamericano. Otro caso interesante de StableCoin es *Finality* [\[2003\]](#), una moneda digital que será emitida en 2020 por un consorcio de bancos para transacciones mayoristas interbancarias, respaldada por UBS, Barclays, Banco Santander, BNY Melln, CIBC, Commerzbank, Credit Suisse, ING, KBC Group, Lloyds Banking Group, MUFG Bank, Nasdaq, Sumitomo Mitsui Banking Corporation y State Street. Esta moneda estable está respaldada por reservas en efectivo en cinco divisas: Dólar Norteamericano, Dólar Canadiense, Libra, Yen y Euro.

Pero también comienzan a verse monedas digitales directamente emitidas por Bancos Centrales, carrera en la que aparentemente China largó primera, en lo que se conoce como Digital Currency Electronic Payment (DCEP) que correrá en *blockchain*, y busca sustituir las monedas y papeles físicos. Esta moneda digital tendrá una paridad 1 a 1 con la moneda nacional (RMB). Sea

utilizando StableCoins, o DCEPs, el próximo paso es automatizar los pagos y liquidaciones a inversores que compren bonos verdes en *blockchain*, mediante *Smart Contracts* que reduzcan el riesgo y los costos asociados a tales operaciones.

5.2.3.3.3.8. Pruebas de Impacto: *off-chain* vs. *on-chain* + *real time* + *on line*

El proceso actual de certificación del impacto de los bonos verdes está delegado a terceros idóneos que realizan auditorías *off-chain* durante el ciclo de vida del proyecto, informando a los inversores sobre el impacto ambiental del proyecto financiado con el bono. En este sentido, el marco armonizado para reportes de impacto de la ICMA [\[2004\]](#) ilustra distintos mecanismos, formularios y métricas de impacto asociadas a los bonos verdes que financian proyectos de energías renovables [\[2005\]](#), de eficiencia energética [\[2006\]](#), agua y gestión de aguas residuales [\[2007\]](#), gestión de residuos [\[2008\]](#), transporte sustentable [\[2009\]](#), y edificios sustentables [\[2010\]](#).

Ahora bien, afirma la S DFA que la gran oportunidad que *blockchain* - combinada con IoT y AI- viene a posibilitar es eliminar al tercero intermediario que audita *off-chain* la performance del activo verde, reemplazándolo por series de datos tokenizados *on-chain*, trazables, recolectados por sensores estratégicamente instalados en la activo verde financiado, que se muestran directamente en la billetera digital del inversor, en tiempo real [\[2011\]](#). Sea mediante monitoreo por cámaras, o chips introducidos en el activo verde que envían datos tokenizados a la *blockchain*, es posible construir reputación sobre el activo verde creando un vínculo directo entre el inversor y el activo financiado.

En efecto, la prueba de impacto tokenizada ya está siendo utilizada por el Programa de Desarrollo de Naciones Unidas (UNDP) en un proyecto sustentable de reforestación bautizado CedarCoin [\[2012\]](#) en el Líbano. El proyecto financia la reforestación de cedros vinculando cada CedarCoin que adquiere un donante a un nuevo cedro plantado. Cada donante puede ver

imágenes del árbol que financió y su ubicación precisa vía coordenadas de GPS. Las personas encargadas del cuidado de los nuevos árboles plantados reciben tokens a cambio (“Clean Air Life Tokens”), que pueden ser cambiados por DAIStableCoins [\[2013\]](#) y por bienes y servicios locales. La prueba de impacto es el oxígeno generado por cada nuevo árbol plantado.

5.2.3.3.3.9. Trazabilidad en la utilización de fondos

Sostiene Richard Posner que la confianza es un sustituto imperfecto de la información [\[2014\]](#) (hermosa frase, por cierto).

Pues bien, es quizás en este tópico donde *blockchain* emerge como una tecnología imbatible, al permitir que los inversores puedan tener una visibilidad y trazabilidad total del uso de los fondos recaudados por el bono verde emitido, si el bono recurre a una StableCoin en su ciclo de vida. Como se indicó más arriba, CNV recomienda que los fondos recaudados por Valores Negociables SVS sean “*asignados a cuentas específicas, u otros mecanismos confiables que garanticen la trazabilidad y la transparencia en el uso de los fondos*”, de modo tal que “*los ingresos netos se pueden acreditar a una subcuenta, o rastrearse de otra manera apropiada*”.

Las tecnologías DLT en general, y *blockchain* en particular, permiten generar un registro inmutable del uso de activos tokenizados al efecto, o lo que es lo mismo, trazar los fondos recaudados y su aplicación mediante *data tokens*. Así, los distintos datos asociados al bono (i.e., monto de suscripción, utilización de fondos, flujos de pagos al inversor, métricas de impacto, etc.), como cualquier otro activo, pueden ser tokenizados y colocados en una *blockchain*, pública o privada permitida a ciertos nodos que pueden accederla (i.e., inversores, reguladores).

Se concuerda con la opinión que afirma que la *blockchain* facilitará un cambio de paradigma, por el cual el dueño del dato, lo controlará end-to-end [\[2015\]](#); en lugar de entregarlo gratuitamente a plataformas que lo monetizan a veces en modos poco éticos. Este cambio de paradigma impactará profundamente en el mercado de capitales, tanto en instrumentos

de renta fija como de renta variable.

5.2.3.3.3.10. *Nodos para supervisores bursátiles*

Si realmente se desea potenciar las Finanzas Sustentables y apalancarlas en las nuevas tecnologías para desatar todo su potencial, los supervisores bursátiles deben estar dentro de la ola, o dicho en términos más tecnológicos, deben ser un nodo que pueda tener acceso al historial de transacciones inmutable, para poder auditarlo en caso de ser necesario. En efecto, la instalación de un nodo por el cual el supervisor -CNV en el caso Argentino- pueda tener acceso a la arquitectura de la *blockchain* en la cual se despliega un bono, sea o no verde, social o sustentable, aumenta la transparencia, despeja riesgos asociados al costoso proceso de KYC, y promueve la más rápida incorporación de tecnología a los servicios financieros. En este sentido, la *blockchain* consorciada como R3 de Corda ya prevé nodos para reguladores que les permiten acceder a cierta información -nodos de observador- [\[2016\]](#).

5.2.3.3.3.11. *La imperiosa necesidad de democratizar la inversión de impacto alineada a los ODS*

Finalmente, otra gran virtud de la *blockchain* aplicada a los bonos verdes alineados a los ODS, es la denominada *fractional ownership*, que permite que un bono verde sea dividido en muchas unidades pequeñas, que pueden ser adquiridas por inversores minoristas, ofreciendo así una nueva oportunidad sustentable para dirigir los ahorros de las personas comprometidas con los ODS, acelerando de este modo las Finanzas Climáticas [\[2017\]](#).

Los signos de los tiempos indican que es esencial para la supervivencia humana agilizar y democratizar el proceso de inversión de impacto alineada a los ODS, ampliando tanto la base de proyectos invertibles como de inversores. Para esta misión tan particular, la cadena de bloques está llamada a jugar un rol trascendental y quizás sea conveniente establecer un *sand-box* dedicado a negocios alineados con los ODS, que permita experimentar con instrumentos de financiación de proyectos sustentables.

A modo de cierre de este apartado, y antes de ingresar a la regulación puntual de los criptoactivos, puede sostenerse que el sistema financiero, compuesto por el mercado monetario y el mercado de capitales, ha experimentado algunas importantes innovaciones jurídicas en los últimos quince años. Sin embargo, más innovación es necesaria, especialmente para financiar esquemas de adaptación y mitigación al cambio climático, el verdadero desafío de nuestros tiempos.

Sin embargo, para que la innovación tecnológica pueda ser utilizada y permita desatar todo el valor que contiene, antes es necesaria la innovación jurídica para dar cabida a nuevas realidades. Como afirmó con toda razón el Maestro Alegría, nuestra cultura jurídica no sólo no puede quedar encandilada por grandes luces, sino que está encomendada a usar el ingenio para recibir y mejorar lo que se decante de precedentes computables, debiendo desarrollar la *ars combinatoria* que requiere de una inventiva propia, de una generación de nuevos recursos técnicos que sirvan para nuestras comunidades en el actual estado de su desarrollo.

5.3. Avances regulatorios: perspectiva comparada

Se han visto en general en el Capítulo III –§ 3.3 y 3.4– algunas posturas regulatorias y legislativas comparadas, que han abordado distintos usos *legalizados* de la *blockchain*, de los criptoactivos, e incluso, del uso de contratos inteligentes en ámbitos muy específicos, como los analizados en § 3.2.2.2 –*smart derivatives contracts*– y § 3.4.2.2.2 –con las *blockchain-based limited liability companies*.

Toca ahora profundizar en la percepción y en la acción tomada por parte de los reguladores más importantes del mundo sobre la *blockchain*, los criptoactivos y los contratos inteligentes.

5.3.1. Commodities vs. ICOs vs. STOs

El impacto de la innovación *on-chain* ha sido particularmente fuerte en tres ámbitos: (i) el bursátil-financiero –a través de los STOs, ICOs, DAICOs y IEOs–; (ii) el bancario comercial –a través de préstamos de criptoactivos que

compiten con los préstamos en dinero fiduciario– y también en la banca de inversión –a través de los smart derivative contracts–; y (iii) también el monetario a través de las CBDCs, StableCoins y Bitcoin.

En consecuencia, los primeros abordajes regulatorios han venido normalmente –aunque no en todos los casos– de la mano de los reguladores bursátiles y de los bancos centrales actuando juntos, como bien ilustra el caso español analizado más arriba en § 3.1.1.1, y también por otros reguladores que supervisan otros ámbitos, como los derivados, la inteligencia financiera – como ha sido el caso de la UIF en 2014 en Argentina, visto en § 3.5.1–, o los servicios de transferencia de dinero. Se dan a continuación algunas precisiones sobre tales avances de los entes reguladores competentes.

5.3.1.1. Directrices sobre token sales de la SEC

Se ha sostenido con toda razón que, en general, las normas que rigen la oferta pública de títulos valores no estaban preparadas para gestionar los atributos de las distintas formas de tokenización, que ofrecen un mercado descentralizado, con liquidez y transferibilidad inmediata a nivel global con solo un click [\[2018\]](#).

En EE.UU, la SEC ha tenido varias oportunidades de fijar su criterio, como se vio en su reporte del caso *TheDAO* en § 2.6.1.1 y en la definición de *securities* que la SEC aplica, vista en § 3.3.1.5.3, que incluye todo contrato de inversión.

Así, en Diciembre de 2017, el Presidente de la SEC [\[2019\]](#) sostuvo que la SEC intentaba establecer una regulación específica en la materia que, a la vez, impulse la innovación responsable y proteja a los inversores y a los mercados. Finalmente, en Abril de 2019, la SEC publicó sus *Guidelines* sobre tokens [\[2020\]](#), muy criticadas por la comunidad *blockchain* ya que, se afirma, no aportó mucha claridad y repitió lo que las leyes y fallos ya dicen [\[2021\]](#).

Se trata de unos lineamientos no vinculantes, que introducen algunos conceptos nuevos. Uno de esos conceptos es el de *Participante Activo* (AP), definido como todo promotor, sponsor o tercero que provee servicios

manageriales que pueden afectar el éxito del emprendimiento, y gracias a los cuales los potenciales inversores pueden pensar que obtendrán beneficios. Conceptos ya familiares, por el *Howey Test*. Afirmó la SEC:

“We recognize that holders of digital assets may put forth some effort in the operations of the network, but those efforts do not negate the fact that the holders of digital assets are relying on the **efforts of the AP**. That a scheme assigns “nominal or limited responsibilities to the [investor] does not negate the existence of an investment contract.” SEC v. Koscot Interplanetary, Inc., 497 F.2d 473, 483 n.15 (5th Cir. 1974) (citation and quotation marks omitted). If the AP provides efforts that are “the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise,” and the **AP is not merely performing ministerial or routine tasks**, then there likely is an investment contract. See Turner, 474 U.S. at 482; see also The DAO Report (although DAO token holders had certain voting rights, they nonetheless reasonably relied on the managerial efforts of others). **Managerial and entrepreneurial efforts typically are characterized as involving expertise and decision-making that impacts the success of the business or enterprise through the application of skill and judgment.**”^[2022] (el resaltado es mío).

Estas Directrices contienen algunos párrafos que parecen comprender la taxonomía propia del token funcional –utility token–, sin embargo, no han fijado un único criterio claro que indique cuándo un token determinado queda afuera de su competencia regulatoria. En efecto, puede leerse:

“Although no one of the following characteristics of use or consumption is necessarily determinative, the stronger their presence, the less likely the Howey test is met:

- The distributed ledger network and digital asset are **fully**

developed and operational.

- Holders of the digital asset are **immediately able to use it for its intended functionality** on the network, particularly where there are built-in incentives to encourage such use.
- The digital assets' creation and structure is **designed and implemented to meet the needs of its users, rather than to feed speculation as to its value** or development of its network. For example, the digital asset can only be used on the network and generally can be held or transferred only in amounts that correspond to a purchaser's expected use.
- **Prospects for appreciation in the value of the digital asset are limited.** For example, the design of the digital asset provides that **its value will remain constant or even degrade over time**, and, therefore, a reasonable purchaser would not be expected to hold the digital asset for extended periods as an investment.

With respect to a digital asset referred to as a virtual currency, **it can immediately be used to make payments** in a wide variety of contexts, or acts as a substitute for real (or fiat) currency. This means that it is possible to pay for goods or services with the digital asset without first having to convert it to another digital asset or real currency. If it is characterized as a virtual currency, **the digital asset actually operates as a store of value that can be saved**, retrieved, and exchanged for something of value at a later time.

With respect to a digital asset that represents rights to a good or service, **it currently can be redeemed within a developed network** or platform to acquire or otherwise use those goods or services. Relevant factors may include:

There is a correlation between the purchase price of the digital asset and a market price of the particular good or service for which it may be redeemed or exchanged.

The digital asset is available in increments that correlate with a consumptive intent versus an investment or speculative purpose.

An intent to consume the digital asset may also be more evident if the good or service underlying the digital asset can only be acquired, or more efficiently acquired, through the use of the digital asset on the network.

- Any economic benefit that may be derived from appreciation in the value of the digital asset is **incidental** to obtaining the right to use it for its intended functionality.
- The digital asset is **marketed in a manner that emphasizes the functionality of the digital asset, and not the potential for the increase in market value of the digital asset.**
- Potential purchasers have the ability to use the network and use (or have used) the digital asset for its intended functionality.
- **Restrictions on the transferability of the digital asset are consistent with the asset's use and not facilitating a speculative market.**
- If the AP facilitates the creation of a secondary market, transfers of the digital asset may only be made by and among users of the platform.”[\[2023\]](#) (el resaltado es mío).

Junto con la emisión de estas Directrices, la SEC publicó también su primera *no-action letter* –una especie de compromiso de no iniciar acciones legales– en un caso de una empresa dedicada a tokenizar millas de vuelo, llamada TurnKey Jet, Inc [\[2024\]](#).

La empresa se dedica a ofrecer servicios de vuelos chárter y taxi aéreo. La empresa decidió ofrecer para la venta tokens convertibles en servicios de vuelos chárter, donde cada token será equivalente a 1 U\$D. Los tokens no son reembolsables. La SEC obligó a la empresa a que (i) los fondos recaudados por la venta de tokens no sean utilizados para desarrollar la plataforma ni la app; (ii) los tokens tienen que ser usables de manera inmediata; (iii) mantengan la paridad 1 token = 1 U\$D; (iv) sólo pueden ser canjeables por servicios aéreos; (v) el emisor *no puede anunciar* o publicitar que los tokens tendrán algún potencial de generar ganancias [\[2025\]](#); y (vi) los tokens sólo

pueden ser intercambiados con otros clientes de la misma empresa, y no pueden “salir” de la plataforma en que se negocien.

Más allá de las Directrices, la SEC ha seguido con su *enforcement*. En Febrero de 2020, se tranzó una demanda civil iniciada por la SEC contra una empresa con base en San Francisco e Israel que ofreció y vendió en una ICO en 2017 75 millones de tokens recaudando 45 millones de Dólares [\[2026\]](#). La empresa aceptó devolver los fondos recaudados a los inversores, y registrar los tokens. Sostuvo la SEC en este caso:

“Enigma and its promoters told investors that Enigma would use the funds raised in the ICO to develop a digital asset trade-testing platform (the “Catalyst Application”) and to **build a data marketplace for cryptocurrency-related data**. Ultimately, as Enigma told investors, Enigma also planned to use ICO funds to develop a marketplace for other forms of data as well (the “Enigma DataMarketplace” or “DataMarketplace”). Based on the facts and circumstances set forth below, **ENG Tokens were offered and sold as investment contracts**, and therefore securities, pursuant to SEC v. W.J. Howey Co., 328 U.S. 293 (1946)”. [\[2027\]](#) (el resaltado es mío).

En Septiembre de 2019, se trazó otra demanda iniciada por la SEC en contra de otra empresa que lanzó una ICO sin previamente registrarse, Block.one, que recaudó varios miles de millones de Dólares entre Junio de 2017 y Junio de 2018 vendiendo 900 millones de tokens. La empresa acordó pagar una multa de 24 millones de Dólares [\[2028\]](#).

Más allá del esfuerzo honesto de la SEC (y de otros reguladores bursátiles en todo el mundo) por proteger a los inversores, uno debe detenerse a pensar la gran velocidad con la que esta tecnología se está moviendo: solo han pasado 5 años entre el primer ICO, *Mastercoin* [\[2029\]](#), creada por un ingeniero de software, J. R. Willet en 2013 y que recaudó 5 millones de Dólares en bitcoins, y la ICO lanzada por Telegram en Enero de 2018, que vendió 2.9 billones de

su token *Gram* a través de SAFTs [\[2030\]](#) y recaudó 1.700 millones de Dólares [\[2031\]](#) para financiar capital de trabajo, su aplicación Telegram y el desarrollo de una *blockchain* propia, *Telegram Open Network* [\[2032\]](#), y que está librando una batalla sin cuartel con la SEC mientras estas líneas se escriben [\[2033\]](#). Y no olvidemos el caso de *Libra*, que casi vio la luz en 2019...

Por otro lado, la postura de la SEC no es distinta cuando los tokens se entregan de manera gratuita a través de *airdrops*. Así, en el caso Tomahawk [\[2034\]](#), la SEC pidió judicialmente una orden de cese en contra de un emisor de ICOs que ofrecía *recompensas* en tokens para quienes denunciaran defectos o *bugs* de programación del *Smart Contract* involucrado. Se sostuvo:

“...the SEC published a cease-and-desist order (the “Tomahawk Order”) focusing, among other things, on a **token issuer that had instituted a token bounty program to promote its ICO**. While the issuer, Tomahawk, “did not raise any money through” and, ultimately, abandoned its planned ICO, Tomahawk nonetheless issued, pursuant to its “Bounty Program,” more than 80,000 TOM tokens to third parties who had assisted in marketing the token, whether using social media or otherwise. Having first determined that the **TOM token was an equity security** the SEC stated that “[t]he ICO and Bounty Program constituted an offer of securities” under the Securities Act, “because it involved ‘an attempt or offer to dispose of, or solicitation of an offer to buy, a security or interest in a security, for value.’” Moreover, the SEC’s analysis clarified that the **token giveaway was, in fact, a sale of securities**, stating: “the distribution of TOM pursuant to the Bounty Program constituted sales under Section 2(a)(3) of the Securities Act, which applies to “every disposition of a security or interest in a security, for value.” Explaining that “**a ‘gift’ of a security is a ‘sale’ within the meaning of the Securities Act when the**

donor receives some real benefit,” the SEC made clear that “the lack of monetary consideration for ‘free’ shares does not mean there was not a sale or offer for sale for purposes of Section 5 of the Securities Act.” Rather, the analysis turns on whether the token issuer received real benefit or value. The SEC determined that Tomahawk “received value in exchange for the bounty distributions, in the form of online marketing,” as well as “in the creation of a public trading market” for the TOM tokens. Specifically, the SEC stated that “[d]istribution of tokens that are securities in exchange for promotional services to advance the issuer’s economic objectives or create a public market for the securities constitute sales” for purposes of both the Securities Act and the Exchange Act (including Rule 10b-5 thereunder) (...) the Tomahawk Order raises at least one thorny related question: Where is the line between a token recipient doing work to “earn” a token, on the one hand, and providing value or benefit to a token issuer, on the other hand?”^[2035] (el resaltado es mío).

Evidentemente, la divisoria de aguas entre security y utility tokens no es muy clara ni en EE.UU ni en la mayoría de los países que han abordado el asunto, con las notables excepciones de Suiza , desarrollada en § 3.4.4.1, y de Francia en § 3.4.8.1.

A todo evento, hasta tanto la legislación aclare el punto, es recomendable que cualquier empresa que decida encarar un proceso de venta masiva de tokens, considere previamente consultar con el regulador bursátil de las jurisdicciones a donde el token será ofertado. Ello así ya que la consecuencia de un eventual encuadramiento como oferta pública irregular pueden incluir, en ocasiones, reproches penales. Evidentemente, la oferta pública tiene sus ventajas, pero dado el caso, la colocación privada de tokens también puede servir a los fines de recaudar fondos para el desarrollo.

5.3.1.2. IOSCO y las plataformas de trading de criptoactivos

En Mayo de 2019, la *International Organization of Securities Commissions* (IOSCO) publicó un documento de trabajo donde aborda específicamente la situación de los *Exchanges* [\[2036\]](#) que crean el mercado secundario para los criptoactivos.

IOSCO los define como *crypto-asset trading platforms*, CTPs. Se analizaron siete aspectos vinculados a los CTPs: (i) acceso al CTP, (ii) custodia de activos de los participantes de CTPs, (iii) conflictos de interés, (iv) operación del CTP, (v) integridad del mercado, (vi) formación de precios y (vii) tecnología.

Estos aspectos se vinculan a tres principios que guían la intervención de los reguladores bursátiles: la protección del inversor, garantizar que los mercados funcionan adecuadamente, de manera justa, eficiente y transparente, y la reducción del riesgo sistémico [\[2037\]](#). A su vez, específicamente en relación a los mercados secundarios, los principios que IOSCO aplica son:

“IOSCO Principle 33 - The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.

IOSCO Principle 34 - There should be ongoing regulatory supervision of exchanges and trading systems which should aim to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.

IOSCO Principle 35 - Regulation should promote transparency of trading.

IOSCO Principle 36 - Regulation should be designed to detect and deter manipulation and other unfair trading practices.

IOSCO Principle 37 - Regulation should aim to ensure the proper management of large exposures, default risk and market disruption. [\[2038\]](#)”

Se definen también cuatro principios que aplican a los intermediarios:

“IOSCO Principle 29 – There should be minimum entry standards for market intermediaries.

IOSCO Principle 30 - There should be initial and ongoing capital and other prudential requirements for market intermediaries that reflect the risks that the intermediaries undertake.

IOSCO Principle 31 - Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting the interests of investors and their assets and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.

IOSCO Principle 32 - There should be procedures for dealing with the failure of a market intermediary in order to minimize damage and loss to investors and to contain systemic risk.

IOSCO Principle 38 - Securities settlement systems and central parties should be subject to regulatory and supervisory requirements that are designed to ensure that they are fair, effective and efficient and that they reduce systemic risk. [\[2039\]](#)„

Se define a las CTPs como:

“a facility or system that brings together multiple buyers and sellers of crypto-assets for the purpose of completing transactions or trades. While CTPs perform functions that are similar to Trading Venues, they may also perform functions that are more typically performed by intermediaries, custodians, transfer agents and clearing houses.” [\[2040\]](#)

5.3.1.3. *Directrices de la Financial Crimes Enforcement Network (FinCEN)*
[\[2041\]](#)

Se ha visto muy someramente el rol activo de FinCEN en § 4.5.6 al tratar el caso *Cryptsy* y en § 3.2.1.2 al tratar el caso *Ripple*.

Corresponde ahora profundizar un poco más. FinCEN depende del Departamento del Tesoro de EE.UU, y es la autoridad de aplicación de la *Currency and Financial Transactions Reporting Act* de 1970, modificada en el año 2001 por la llamada *USA PATRIOT Act*, y aplica en general la legislación conocida como *Bank Secrecy Act* (“BSA”), que contiene las normas de AML y counter-terrorism financing (CTF), a nivel Federal en EE.UU^[2042]. *Mutatis mutandis*, es el equivalente funcional de la Unidad de Información Financiera (UIF). Además de la legislación federal, en EE.UU existe una frondosa legislación sub-nacional que regula la transmisión de dinero, pero está enfocada en la protección del consumidor y no en AML-CFT^[2043].

La BSA obliga a las instituciones financieras –bancos, brokers de títulos valores, *money services business*, casinos, etc.– a que vigilen la conducta financiera de sus clientes, incluyendo la presentación de reportes de operación sospechosa y la generación de *currency transaction reports* (CTRs). Los *money services business*, que incluyen a las empresas que hacen envíos de dinero, son las entidades más vigiladas, y se los define como:

“(a) [a]ny person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or

(b) [a]ny other person engaged as a business in the transfer of funds. The term “money transmission services” means “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another

location or person by any means.”^[2044] (el resaltado es mío).

En 2013, FinCEN emitió sus *Directrices* sobre monedas virtuales, afirmando que aplicaría a las monedas virtuales las mismas normas que se aplican al dinero fiduciario^[2045]. Definió allí a las *convertible virtual currency*:

“having “an equivalent value in real currency, or acts as a substitute for real currency.” FinCEN regulations cover both transactions where the parties are **exchanging fiat and convertible virtual currency**, as well as transactions **from one virtual currency to another virtual currency**. **Businesses providing anonymizing services** (also known as “mixers” or “tumblers”), which attempt to conceal the source of the transmission of virtual currency, are money transmitters when they accept and transmit convertible virtual currency and, therefore, have regulatory obligations under the BSA (...) **The convertibility of the virtual currency is an important distinction**. If a virtual currency cannot be converted to or sold for real currency and does not have any monetary value on the open market, then it does not implicate federal money transmission laws.”^[2046]

Las Directrices de FinCEN definen a los usuarios^[2047], a los *Exchangers*^[2048], y a los Administradores^[2049]. Los últimos dos están sujetos a obligaciones de registro y deben obtener una licencia para operar. Luego de estas primeras directrices generales de 2013, se dictaron tres más particularizadas en 2014, enfocadas en los desarrolladores de software y ciertas actividades de inversión, la minería, y los servicios de pagos en criptoactivos^[2050].

Este combo regulatorio define en qué condiciones la actividad requiere una licencia previa de FinCEN, definiendo a los desarrolladores de software

aplicado a criptoactivos [\[2051\]](#), a los mineros [\[2052\]](#), a las monedas virtuales centralizadas [\[2053\]](#), las monedas virtuales descentralizadas [\[2054\]](#), *Wallets* [\[2055\]](#), *Exchanges* [\[2056\]](#), y a los desarrolladores de tokens [\[2057\]](#).

En Mayo 2019, FinCEN emitió unas nuevas Directrices [\[2058\]](#) donde abordó específicamente el caso de las ICOs, en dos supuestos usuales, y fijó su criterio en estos términos:

“Initial coin offerings (ICOs) are generally a means to raise funds for new projects from early backers. **Whether an ICO is subject to BSA obligations is a matter of facts and circumstances.** This guidance will address, as an example, the BSA obligations of two common business models involving ICOs: (a) **ICOs conducting a preferential sale of CVC to a select group of buyers** (sometimes referred to as investors); and (b) **ICOs raising funds by offering digital debt or equity instruments among a group of lenders or investors to finance a future project** (which in turn may consist of the creation of a new CVC) (...). In the first business model, the ICO consists of a group sale of CVC to a distinct set of preferred buyers. The exchange of CVC for another type of value may be instantaneous or deferred to a later date. The CVC and its application or platform may be already operational or it may be the seller’s purpose to use the value received from the sale, in whole or in part, to develop such CVC, application, or platform. In some cases, after the initial centralized offering, any future creation of the CVC may occur through mining using a decentralized model. In any of these scenarios, **the seller of the CVC is a money transmitter, acting in the role of administrator**, because at the time of the initial offering the seller is the only person authorized to issue and redeem (permanently retire from circulation) the new units of CVC. The status of the seller as a money transmitter is not impacted

by the coordinated or simultaneous sales; the timing of acceptance of one type of value and transmission of the other type (i.e., whether the exchange happens instantaneously or at a later date); or by the fact that the payment system may migrate from one operational status to another at any point in its lifetime (for example, changing from a centralized, administrator-controlled system at origin to a decentralized, protocol-driven system after the initial sale) (...) **In the second business model, the ICO raises funds for new projects by selling an equity stake or a debt instrument to early backers,** or hedges a previous investment in CVC through a derivative, such as a futures contract. The funded project generally involves the creation of DApps, new CVCs (as well as the applications or platforms on which the CVCs will run), or new hedging instruments. ICOs are accomplished using distributed ledger platforms, in which **investors receive a digital token as proof of investment.** Depending on the purpose of the funded project and the seller's obligations to the investor, when the project is concluded the investor may: (a) receive new CVC in exchange for the token; (b) exchange the token for a DApp coin, which is a digital token that unlocks the use of DApps that provide various services; (c) use the original token itself as a new CVC or DApp coin; or (d) receive some other type of return on the original equity investment or debt instrument (...) a person involved in ICO fundraising activity as issuer, intermediary, or investor that is a **bank, foreign bank, or a person registered with, and functionally regulated or examined by the SEC or CFTC will not be an MSB under FinCEN regulations** (...) FinCEN regulations exempt persons from the definition of money transmitter under certain identified facts and circumstances, the most relevant of which is when the **acceptance and transmission of value is only integral to the sale of goods or services different from money transmission.** Thus, if the person involved in the fundraising activity as an issuer, intermediary, or investor is not a bank, foreign bank, or a person registered with, and functionally

regulated or examined by the SEC or CFTC, then any money transmission connected to the fundraising activity performed by the person generally will fall under the integral exemption, **unless the asset is issued to serve as value that substitutes for currency** (...) The investor may hold the digital token or derivative until the underlying project is complete, or the investor may sell the digital token or derivative during the project's development. A re-sale can occur through a P2P transaction, or through a financial intermediary or secondary market. **In general, the re-sale of the token or derivative does not create any BSA obligations for the initial investor**". (el resultado es mío).

En cuanto al desarrollo de Dapps financiado vía ICOs, FinCEN considera:

"The development of a DApp financed through ICO fundraising activity consists of the production of goods or services, and therefore **is outside the definition of money transmission**. Thus, **the developer of a DApp is not a money transmitter for the mere act of creating the application**, even if the purpose of the DApp is to issue a CVC or otherwise facilitate financial activities denominated in CVC. **However, if the developer of the DApp uses or deploys it to engage in money transmission, then the developer will qualify as a money transmitter under the BSA**. Once the DApp is finalized and in production, FinCEN regulations may apply to persons who use the DApp to conduct certain financial activities. For example, if an investor or an owner/operator uses or deploys the DApp to engage in money transmission denominated in CVC, then the investor or the owner/operator generally qualifies as a money transmitter under the BSA. Likewise, as mentioned above, if the developer of the DApp uses or deploys the DApp to engage in money transmission, then the developer will also qualify as a money transmitter."^[2059] (el resultado es

mío).

FinCEN también aborda el caso de creadores de CVCs:

“The creators of a CVC sometimes issue (or “pre-mine”) a certain number of CVC units in advance and then either distribute those units as payment for goods or services or repayment of obligations (such as amounts owed to project investors), or sell the units against currency, funds or another type of CVC once a market is established. **To the extent that a person mines CVC and uses it solely to purchase goods or services on its own behalf, the person is not an MSB under FinCEN regulations**, because these activities involve neither acceptance nor transmission of the CVC within the regulatory definition of money transmission services. However, **if a person mines CVC and uses it to engage in money transmission, such person will be subject to FinCEN’s registration**, reporting, monitoring, and recordkeeping regulations for MSBs, as is the case with all money transmitters. [\[2060\]](#)” (el resaltado es mío).

Finalmente, FinCEN también aborda el caso de los procesadores de pagos que utilizan CVCs y de los cajeros –ATMs– que cambian dinero fiduciario por monedas virtuales :

“Virtual currency payment processing systems typically process payments and assist in executing transactions by accepting cash from the buyer, keeping that cash, and then paying the seller with the approximate market value of a virtual currency, or vice versa. By keeping a large reserve of virtual currency at all times, the payment processor is able to act as his/her own currency exchange to supply equivalent virtual currency for the cash supplied by the buyer. According to FinCEN, **payment**

processing systems that accept and convert both real and virtual currencies are money transmitters because they are exchangers and, therefore, must register. “An exchanger will be subject to the same obligations under FinCEN regulations regardless of whether the exchanger acts as a broker (attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another) or as a dealer (transacting from its own reserve in either convertible virtual currency or real currency). There is, however, a carve-out from registration for payment processors when four conditions are met: (a) the entity providing the service facilitates the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself); (b) the entity operates through clearance and settlement systems that admit only BSA-regulated financial institutions; (c) the entity provides the service pursuant to a formal agreement; and (d) the entity’s agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds. Bitcoin ATMs, however, are not merely an intermediary between a consumer and his/her personal bank. **Bitcoin ATMs function as either one-way (converting fiat currency to Bitcoin) or two-way (converting fiat currency to Bitcoin and Bitcoin to fiat currency) machines. In both instances, these machines may act as intermediaries between buyers and sellers, more as a broker than as a teller. Therefore, Bitcoin ATM operators generally must register with FinCEN as money transmitters.**”^[2061] (el resaltado es mío).

5.3.1.4. La auto-regulación de los intermediarios: Financial Industry Regulatory Authority (FINRA)

FINRA es una asociación privada de EE.UU que nuclea y auto-regula a los brokers y mercados de valores como el NYSE y el NASDAQ y que se

encuentra bajo supervisión de la SEC, que puede invalidar las regulaciones auto-impuestas por FINRA. Una empresa que desee ofrecer servicios de intermediación de criptoactivos en EE.UU, debe registrarse en FINRA.

En Junio de 2019, más de 40 intermediarios en criptoactivos denunciaban demoras de hasta 14 meses en conseguir las autorizaciones para operar [\[2062\]](#).

En un informe de 2017, FINRA puntualizaba los requerimientos esenciales que debieran ser cumplidos por intermediarios de criptoactivos [\[2063\]](#):

“Broker-dealers handling customer funds and securities are subject to a number of requirements, including **Rule 15c3-3 under the Securities Exchange Act of 1934** (Exchange Act). The SEC has previously stated that one of the key requirements imposed by Rule 15c3-3 is that “the **broker-dealer must maintain physical possession or control over customers’ fully paid and excess margin securities.**” Securities transactions entered into, cleared and settled using DLT may also have implications for firms’ obligations under **Exchange Act Rule 15c3-1 related to net capital requirements** (...) Similarly, if any cash-backed token holdings or digital currency were used as part of a DLT application, **broker-dealers would need to consider how this would affect their processes for complying with requirements under Rule 15c3-3, including the customer and proprietary account reserve formulas** (...) Broker-dealers would also need to consider how they would comply with **asset verification requirements**, such as under FINRA Rule 4160 (Verification of Assets) and Exchange Act Rule 17a-13, in the context of DLT applications resulting in the use of cryptosecurities. Broker-dealers are subject to **recordkeeping requirements** under Exchange Act Rules 17a-3 and 17a-4 and FINRA Rule 4511 (Books and Records: General Requirements), which outline minimum requirements regarding the **types of records that must be made, as well as the length of time that broker-dealers must maintain**

relevant records and other documents pertaining to their business (...) Depending on how trade execution and settlement is ultimately structured, broker-dealers and other market participants may wish to consider whether any of their activities in the DLT environment meet the definition of a clearing agency and whether corresponding clearing agency registration requirements under Section 17A of the Exchange Act would be applicable (...) the development of a DLT environment that alters the **clearing and settlement process** for securities transactions may also impact introducing broker and clearing broker (i.e., the carrying firm) relationships. FINRA Rule 4311 (**Carrying Agreements**) requires, among other things, that “the carrying firm shall submit to FINRA for prior approval any agreement for the **carrying of accounts, whether on an omnibus or fully disclosed basis, before such agreement may become effective.** The carrying firm also shall submit to FINRA for prior approval any material changes to an approved carrying agreement before such changes may become effective (...) The Bank Secrecy Act of 1970 (BSA) requires all broker-dealers to, among other things, implement compliance **programs to detect and prevent money laundering.** In addition, FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires all broker-dealers to **develop and maintain a written AML program to comply with the requirements of the BSA.** The BSA also requires that, as part of the AML program, broker-dealers must establish, document and maintain a reasonable customer identification program (CIP), which, among other things, requires **broker-dealers to verify identities of all parties with which they establish a formal relationship to effect securities transactions (...)** FINRA Rule 2090 (Know Your Customer (KYC)) requires broker-dealers to “use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer (...) As required by Regulation S-P, broker-

dealers must have written policies and procedures in place to address the **protection of customer information and records** (...) Pursuant to various rules, FINRA member firms are obligated to **report certain order-and-trade-related information into these FINRA facilities**. Broker-dealers should be mindful of how such reporting obligations may apply when participating or transacting in a DLT network (...) FINRA Rule 2122 (Charges for Services Performed) requires that any charges for services performed must “be reasonable and not unfairly discriminatory among customers.” Likewise, any commissions or mark-ups on DLT-derived products would be subject to standards outlined in FINRA Rule 2121 (Fair Prices and Commissions).” (el resaltado es mío).

En materia de auto-regulación del ecosistem *blockchain*, téngase presente el importante avance registrado en Japón, visto § 3.4.6, a donde se ha creado la primera asociación de *Exchanges*^[2064] del mundo, constituida con la finalidad de auto-regular al sector^[2065].

5.3.1.5. *Commodity Futures Trading Commission (CFTC)*

En § 4.7.5.4 y § 3.5.1.2.4, se analizaron de manera preliminar algunos posicionamientos regulatorios de la CFTC en el caso *McDonnell*. Corresponde ahora profundizar su enfoque. El primer posicionamiento administrativo de la CFTC es del año 2015, en el caso *Coinflip*^[2066].

5.3.1.5.1. *CFTC vs. Coinflip*

En este caso, la CFCT inició un sumario administrativo contra Coinflip y su fundador, alegando la violación de varias normas que integran la competencia de este regulador, lo que fue reconocido por los sumariados a los fines de transar el procedimiento iniciado. Se sostuvo que los sumariados habían ilegalmente iniciado una plataforma llamada *Derivabit*, donde

ofrecían contratos de opción y swaps sobre bitcoins, sin previamente haberse registrado en la CFTC. Sostuvo la CFTC:

“Beginning in March 2014, Coinflip advertised Derivabit as a “risk management platform that connects buyers and sellers of standardized Bitcoin options and futures contracts.” During this period, Coinflip designated numerous put and call options contracts as eligible for For these contracts, Coinflip listed Bitcoin as the asset underlying the option and denominated the strike and delivery prices in US Dollars. According to the derivabit.com website, a customer could place orders by registering as a user and depositing Bitcoin into an account in the user's name. Premiums and payments of settlement of the option contracts were to be paid using Bitcoin at a spot rate determined by a designated third-party Bitcoin currency exchange. Users had the ability to, and in fact did, post bids or offers for the designated options contracts (...) Derivabit had approximately 400 users”^[2067]

Dos años después del caso *Coinflip*, en 2017, la CFTC publicó un primer documento de trabajo donde abordada los criptoactivos^[2068]. Allí se sostuvo que:

“The CFTC first found that Bitcoin and other virtual currencies are properly defined as commodities in 2015 . The CFTC has oversight over futures, options, and derivatives contracts. **The CFTC’s jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce.** Beyond instances of fraud or manipulation, **the CFTC generally does not oversee “spot” or cash market exchanges** and transactions involving virtual currencies that do not utilize margin, leverage, or

financing.”^[2069] (el resaltado es mío).

En el documento de 2017, la CFTC comentaba casos que habían sido expresamente autorizados para operar derivados sobre criptoactivos:

“TeraExchange, LLC, a Swap Execution Facility (“SEF”) registered with the CFTC, entered in to the virtual currency market in 2014 by listing a **Bitcoin swap for trading**. Trading on a SEF platform is limited to “eligible contract participants,” a type of sophisticated trader, which includes various financial institutions and persons, with assets above specified statutory minimums.

North American Derivatives Exchange Inc. (“NADEX”), a designated contract market (“DCM”), listed **binary options based on the Tera Bitcoin Price Index from November 2014 to December 2016**. Retail customers may trade on NADEX. LedgerX, LLC (“LedgerX”) registered with the CFTC as a SEF and Derivative Clearing Organization (“DCO”) in July 2017. It plans to list digital currency options.”^[2070] (el resaltado es mío).

En el mismo documento, la CFTC afirmó que estaban prohibidas las siguientes actividades sobre criptoactivos:

“Price manipulation of a virtual currency traded in interstate commerce.

Pre-arranged or wash trading in an exchange-traded virtual currency swap or futures contract.

A virtual currency futures or option contract or swap traded on a domestic platform or facility that has not registered with the CFTC as a SEF or DCM.

Certain schemes involving virtual currency marketed to retail customers, such as off-exchange financed commodity

transactions with persons who fail to register with the CFTC.”
(el resaltado es mío).

Llamativamente, en relación a los desarrolladores de *Smart Contracts*, el Presidente de la CFTC dio un discurso en 2018, donde afirmó:

“In my view, with respect to any Smart Contract protocol, the first step in the analysis is defining the basic nature of the contract. **Is it a contract for sale or a rental agreement? Or, does it have the essential characteristics of a swap, future or option? If so, is the product accessible by U.S. persons?** If the contract is a product within the CFTC’s jurisdiction, then regardless of whether it is executed via a written ISDA confirmation or software code, **it is subject to CFTC regulation.** If the Smart Contract is within the CFTC’s jurisdiction, then the next question becomes, is the method by which it is being transacted on the blockchain compliant with CFTC regulations? If the contract is a swap, is it being offered to retail participants? Is it a product that must be traded on an exchange? Does the protocol itself perform exchange-like functions by facilitating trading, thereby potentially implicating registration requirements? These are all open questions that the CFTC must consider and resolve as Smart Contracts proliferate and perhaps become a common feature of our financial markets.”^[2071] (el resaltado es mío).

Seguidamente, la CFTC emitió a fines de 2018 un informe específico sobre *Smart Contracts*^[2072]. Allí se aclaró como criterio regulatorio que la CFTC tiene el poder de policía sobre:

“Trading Exchanges/Organizations (e.g., Designated Contract Markets (**DCMs**) and Swap Execution Facilities (**SEFs**), and Forward Boards of Trade (**FBOTs**)).

Clearing Organizations (e.g., Derivatives Clearing Organizations (DCOs)).

Data Repositories (e.g., Swap Data Repositories (SDRs)).

Intermediaries (e.g., Futures Commission Merchants (FCMs), Introducing Broker (IBs), Commodity Pool Operators (CPOs), and Commodity Trading Advisors (CTAs)).

Counterparties (e.g., Swap Dealers (SDs))”^[2073] (el resaltado es mío).

Sobre ese amplio universo regulado, la CFTC afirmó que un contrato inteligente puede ser programado de modo tal de ser considerado un *commodity*, o un contrato de forward, o un contrato de futuros, o un contrato de opción o un swap, y todos éstos contratos, y también los commodities, *están dentro del perímetro regulatorio de la CFTC*. En mérito a tal definición, la doctrina norteamericana ha interpretado que los desarrolladores de *Smart Contracts* deben tener en cuenta el ámbito de regulación de la CFTC a la hora de encarar la programación, ya que pueden ser legitimados pasivos de sumarios administrativos y demandas judiciales iniciadas por la CFTC^[2074].

5.3.1.6. El caso de Malta

Malta es un país muy *crypto-friendly*, que amerita un estudio detenido. Ya hace 10 años que se ha convertido en el *hub* de todas las empresas del juego on line europeas, y aspira a convertirse también en un *crypto-hub*^[2075], al igual que el Reino Unido, en § 3.4.1, Francia, como se vio en § 3.4.8 y Suiza en § 3.4.4.1.

En 2018, una coalición institucional guiada por el Parlamento maltés y la Malta Financial Services Authority (“MFSA”) se propuso convertir a la isla en una *Blokchain Island*, y sancionó tres leyes:

- 1) Creó la Malta Digital Innovation Authority (MDIA):
- 2) Sancionó la ley de Servicios y Contratos de la Innovación Tecnológica; y

3) Sancionó la Ley de Activos Digitales: se reconoce el dinero electrónico y a los títulos valores regulados –como regulaciones preexistentes que pueden ser de aplicación–, a los nuevos *utility tokens* digitales, y a los nuevos activos financieros virtuales [\[2076\]](#), y se regulan los *Exchanges* –que necesitan autorización previa para funcionar–, los emisores de *utility tokens*, y a un intermediario nuevo, conocido como *Virtual Financial Asset Agent*, que también debe inscribirse y certificar en todos los casos la naturaleza de los criptoactivos involucrados. Los *utility tokens* quedan afuera de la regulación maltesa.

Sin embargo, a pesar del régimen relativamente sencillo y claro, a Abril de 2020, operaban en la isla 83 emprendimientos del ecosistema *blockchain*. Sólo 26 solicitaron su inscripción en el registro respectivo en el plazo previsto en la nueva legislación, y a la fecha, ninguna autorización ha sido dada [\[2077\]](#). Se publicó desde la MFSA una lista de 57 empresas que debían registrarse, y no lo habían hecho a Abril de 2020 [\[2078\]](#).

5.3.1.6.1. *Utility tokens*

La legislación maltesa los define como:

“a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on, or in relation to which, it was issued or **within a limited network of DLT platforms (but not DLT exchanges).**” [\[2079\]](#) (el resaltado es mío).

5.3.1.6.2. *Activo Financiero Virtual*

Los *Virtual Financial Assets* son los que quedan regulados por un nuevo régimen desde Julio de 2018, un régimen *distinto* a los preexistentes regímenes regulados, del dinero electrónico y de los títulos valores regulados. El emisor de un VFA debe registrar el White Paper en la MFSA, y aplican ciertos lineamientos para la confección de dichos documentos. Los White Papers deben detallar cómo cumplen la legislación maltesa de AML-CTF.

5.3.1.6.3. *El SandBox maltés: gaming & gambling meets the ledger*

En Marzo de 2018, el gobierno maltés dispuso un *SandBox* vinculando a la industria del juego y las apuestas on line con las criptomonedas. En Junio, se lanzó desde la Bolsa de Malta una Aceleradora fintech en sociedad con Thomson Reuters y Binance, enfocada en invertir en startups que apliquen tecnología *blockchain* al mundo financiero. Malta integra la European *Blockchain* Partnership y apuesta fuertemente a vincular el *hub* del juego *on line* con las criptomonedas [\[2080\]](#). Las apuestas ya han llegado a la *blockchain* con monedas nativas digitales, de la mano de la plataforma Augur [\[2081\]](#):

“Augur is a decentralized oracle and peer to peer protocol for prediction markets. Augur is free, public, open source software, portions of which are licensed under the General Public License (GPL) and portions of which are licensed under the Massachusetts Institute of Technology (MIT) license. **Augur is a set of Smart Contracts written in Solidity that can be deployed to the Ethereum blockchain.**” (el resaltado es mío).

5.3.1.7. *Otros enfoques regulatorios*

Para otros enfoques regulatorios, se remite al lector a § 3.4.

5.4. Aspectos fiscales: perspectiva comparada. Tributación en Argentina.

5.4.1. La tributación digital

Se ha conceptualizado a la Economía Digital como la infraestructura de telecomunicaciones, las industrias TIC y la red de actividades económicas y sociales facilitadas por Internet, la computación en la nube, las redes móviles, sociales y de sensores remotos [\[2082\]](#).

Se ha afirmado que es en su ámbito donde la frase “*ingresos sin Estado*” tiene sentido [\[2083\]](#), y donde han nacido los servicios digitales y el comercio electrónico B2B, B2C, C2C, B2G, C2B, y B2B2C.

¿Cómo encuadra toda esta nueva realidad *digital* en las normas impositivas? ¿Cómo juegan los conceptos de residencia fiscal, establecimiento permanente y *establecimiento permanente digital*? Los conflictos fiscales interjurisdiccionales han existido siempre, con tironeos entre fiscos que buscan gravar según el criterio del domicilio *fiscal* de quién obtuvo la renta, con fiscos que buscan gravar según el criterio del domicilio *real* donde se generó la renta, y, siempre, con fiscos que bajan sus impuestos para atraer a los generadores de la renta, siendo icónico el caso de Irlanda [\[2084\]](#), seguida por Suiza, Dinamarca, Suecia y Luxemburgo. Así han nacido los acuerdos de (no) doble tributación internacional [\[2085\]](#).

Por otro lado, países como Noruega, desde 2011, recauda el IVA del 25% sobre servicios digitales, y Méjico estableció un impuesto del 3% a todos los servicios digitales, al igual que Italia [\[2086\]](#).

Todo ello ha motivado que la OCDE elabore un plan de acción sobre BEPS: *Base Erosion and Profit Shifting*. Las BEPS producen un no pago aproximado del 10% en el impuesto a las ganancias global, y totalizaba, se pensaba, 240 mil millones de Dólares anuales ya en 2015 [\[2087\]](#). Sin embargo, en un informe de

Junio de 2019 de la OECD sobre BEPS, las palabras *blockchain* y token están ausentes [\[2088\]](#), y el proyectado *Impuesto sobre Servicios Digitales* de la Unión Europea, aunque sí alcanzará a los *marketplaces*, a los servicios de *streamming*, así como las plataformas de *sharing economy*, y, en general, a servicios que conecten a los usuarios [\[2089\]](#), no está claro si incluirá a los criptoactivos y a las plataformas que conectan a los tenedores de criptoactivos.

5.4.2. Breve perspectiva comparada de la tributación de los criptoactivos [\[2090\]](#)

Empezamos por Australia. En Australia, desde Julio de 2017 las criptomonedas no son consideradas divisas, ni dinero de curso legal, ni servicios financieros, sino que son consideradas un clase de *activo* a los fines del impuesto a las ganancias del capital, *Capital Gains Tax* (CGT) [\[2091\]](#): su venta o disposición tributa igual que la venta de acciones.

Ahora bien, el uso y tenencia de ciertos criptoactivos como medio de pago para la compra de bienes y servicios diarios está exento en el CGT hasta los 10.000 Dólares Australianos –recuérdese que esta excepción que opera como un *mínimo no imponible* también se propuso en EE.UU, en § 3.3.1.1– y también está exento en el *Good and Services Tax*, GST, que no grava el pago de bienes y servicios con ciertas criptomonedas como Ethereum, bitcoin, Litecoin, Dash, Monero, Zcash, Ripple y YbCoin [\[2092\]](#).

En cambio, sí pagan el GST los proveedores de servicios digitales como Netflix, y todos aquellos que se dedican profesionalmente a la venta a terceros de criptoactivos, *Exchanges*. Llamativamente, también se paga GST por la compra de criptomonedas respaldadas por otro valor, ya que no se las considera criptomonedas propiamente dichas. Así, la compra, tenencia y venta de Tether [\[2093\]](#), por ejemplo, tributará CGT y GST, y los utility tokens, tampoco están exentos de GST ya que no son considerados una moneda

digital^[2094]. Por otro lado, el *Income Tax* comprende también a los *Exchanges* y a los mineros que actúan como empresa no personificada.

En el Reino Unido, desde el año 2014 el ente recaudador reconoce que ciertos comercios aceptan bitcoin como pago por sus servicios y bienes vendidos, y también que las personas y empresas poseen ciertos criptoactivos como inversión^[2095].

Desde el punto de vista del *Corporate Tax* (CT) y del *Income Tax*, los criptoactivos son tratados igual que la divisa extranjera, con lo cual las pérdidas y ganancias se tributan del mismo modo que ocurre con una divisa^[2096].

Desde el punto de vista del *Value Added Tax* (VAT), la minería está exenta, y también está exento del VAT recibir bitcoins en pago por mercaderías o servicios, respecto sólo al valor de los bitcoins *per se*, debiéndose tributar el VAT que corresponda al producto o servicio vendido. Se sostiene que “*in all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoin or other similar cryptocurrency. The value of the supply of goods or services on which VAT is due will be the sterling value of the cryptocurrency at the point the transaction takes place.*”^[2097]

En un documento emitido en Diciembre de 2019, el recaudador inglés aclaró ciertos criterios tributarios respecto, específicamente, de los *payment tokens*, a los que denomina *exchange tokens*, y las actividades a ellos vinculadas: *exchanges* y *mining*. Se abordó también los criptoactivos que son producto de *hard* o *soft forks*, los *airdrops*, y el pago de salarios con criptoactivos. Se dejó para otra oportunidad la tributación de los ICOs y STOs, pero se fijaron los criterios tributarios aplicables a seis tributos: VAT, CGT, Corporation Tax, Income Tax, National Insurance Contribution y Sellos^[2098].

En Canadá no se considera a los criptoactivos ni como moneda de curso legal ni como divisa, sino una propiedad imponible, y a la que se aplican las reglas y criterios tributarios que aplican a cualquier activo^[2099]. Desde el

punto de vista del *income tax*, si un comercio acepta criptomonedas como forma de pago, deberá convertir su valor a dinero fiduciario al día de la transacción y pagar la ganancia que corresponda [\[2100\]](#). La tenencia de criptoactivos, por su parte, es considerada igual que la tenencia de un commodity, por lo que habrá ganancia o pérdida según a qué valor se venda, comparado a qué valor se lo compró. La minería está sujeta a impuesto a las ganancias, para lo cual se analizará el inventario del minero al cierre del año fiscal.

En Estonia, por su parte, los criptoactivos desde 2014 son considerados, a los fines fiscales, como un medio de pago alternativo y sujeto a CGT y al VAT. Bitcoin, puntualmente, no es considerado dinero electrónico ni como un título valor [\[2101\]](#).

En Japón, desde 2017, las criptomonedas que son consideradas *virtual currency*, e.g. bitcoins, están exentas en el *Consumption Tax*, pero las ganancias derivadas de la venta de criptoactivos están alcanzadas en el impuesto a las ganancias, con la particularidad que no pueden compensarse tales ganancias contra quebrantos generados por otra fuente, y el impuesto a las herencias grava los criptoactivos [\[2102\]](#).

En EE.UU, a nivel federal, los criptoactivos *convertibles* en dinero fiduciario son considerados una propiedad a los fines del *Income Tax* [\[2103\]](#). Para la IRS:

“A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.

Payments using virtual currency made to independent contractors and other service providers are taxable, and self-employment tax rules generally apply.

Wages paid to employees using virtual currency are taxable to the employee, must be reported by an employer on a Form W-2 and are subject to federal income tax withholding and payroll

taxes.

Certain third parties who settle payments made in virtual currency on behalf of merchants that accept virtual currency from their customers are required to report payments to those merchants on Form 1099-K, Payment Card and Third Party Network Transactions.

The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer. [\[2104\]](#)” (el resultado es mío).

En este sentido, en EE.UU:

“For federal tax purposes, cryptocurrencies are not currencies that can generate foreign currency gains or losses. If a taxpayer receives cryptocurrency as payment for goods or services, they must include the fair market value of the cryptocurrency in US dollars at the date the cryptocurrency was received in their gross income calculations. If the fair market value of property exchanged for cryptocurrency exceeds the fair market value of the cryptocurrency at the time it is received the taxpayer has a taxable gain. Conversely, if the fair market value of the property is less than the fair market value of the cryptocurrency received, the taxpayer has a loss, which may be deductible. Whether a gain or loss is capital gain or loss or an ordinary gain or loss depends on whether the cryptocurrency is a capital asset (such as stocks, bonds or investment property) or not (for example, if cryptocurrency is held as inventory) in the hands of the taxpayer and is taxed accordingly.

Taxpayers who mine cryptocurrencies, such as bitcoin miners, must include the fair value of the cryptocurrency in US dollars in their gross income as at the date the cryptocurrency was received. Cryptocurrency received by an independent contractor for services performed constitutes self-employment

income and is subject to self-employment tax on the fair value of the cryptocurrency in US dollars at the date it is received.

Cryptocurrency paid to an employee by an employer as remuneration constitutes wages and is subject to federal income tax withholding on the fair value of the cryptocurrency in US dollars at the date of payment.

Payments made in cryptocurrencies to a US non-exempt recipient where the fair value of the cryptocurrency is \$600 or more are subject to the same information reporting requirements as any other payment made in property. Such payments could include rent, wages or annuities.

In general, a person who makes a payment in cryptocurrency to an independent contractor for services performed where the fair value of the cryptocurrency is \$600 or more in a taxable year is required to file an information return with the IRS.

Payments made using cryptocurrency are subject to backup withholding to the same extent as other payments made in property. In general, a third party who contracts to settle payments on behalf of unrelated merchants and their customers (a third-party settlement organisation) must include payments made in cryptocurrencies at their fair value in US dollars at the date of payment in aggregation with payments made in real currencies when determining the total amount they are required to report to the IRS”^[2105] (el resaltado es mío).

Es también interesante el enfoque fiscal de Portugal^[2106], que en Septiembre de 2019 eximió de impuestos a las ganancias y al valor agregado a la compra y venta de criptoactivos, al considerarlos una forma de dinero, pero aclarándose que recibir criptoactivos en pago no cambia la posición fiscal de la operación económica subyacente, que estará sujeta a las reglas de tributación ordinarias. Por otro lado, dedicarse profesionalmente a la venta y compra de criptoactivos no es una actividad exenta.

En Colombia, por su parte, se considera que los criptoactivos como bitcoin

tributan impuesto a las ganancias igual que cualquier otro activo de inversión [\[2107\]](#), y no se los considera una divisa, siendo su naturaleza jurídica la de un bien incorporal [\[2108\]](#). Con relación a los mineros, en Colombia se los define como:

“Un minero es una persona o entidad que participa en una red de moneda virtual descentralizada mediante la ejecución de un software especial para resolver complejos algoritmos en una prueba de trabajo distribuida u otro sistema de prueba distribuido utilizado para validar las transacciones en el sistema de moneda virtual. Los mineros pueden ser usuarios, si se autogeneran una moneda virtual convertible únicamente para sus propios fines, por ejemplo: para mantener la inversión, para pagar una obligación existente o para comprar bienes y servicios. Los mineros también pueden participar en un sistema de moneda virtual como intercambiadores, generando moneda virtual como un negocio con el fin de venderla por moneda fiduciaria u otra moneda virtual. [\[2109\]](#)” (el resaltado es mío).

Un proyecto de Ley presentado en 2018, definía a los *Exchange* como:

“Entidades de operaciones con criptomonedas. Son aquellas personas jurídicas con ánimo de lucro o naturales que ejerzan como comerciantes y con establecimientos de comercio inscritos en la Cámara de Comercio, cuyo objeto social sea la comercialización, administración o trading de criptomonedas, con previa autorización emitida por el Ministerio de Tecnologías de la Información y de las Comunicaciones.” [\[2110\]](#) (el resaltado es mío).

Así, en Colombia, para el Impuesto sobre la Renta, las criptomonedas son activos intangibles. Por tal motivo, deben ser reconocidos patrimonialmente

por los contribuyentes en sus declaraciones de impuesto sobre la renta, e incluso en el impuesto al patrimonio. Asimismo, la incorporación y medición de estos debe tener consecuencias en aspectos relevantes para el impuesto sobre la renta, tales como la renta por comparación patrimonial y la renta presuntiva [\[2111\]](#). En consecuencia, para un contribuyente, persona humana no obligada a llevar contabilidad y que lleve a cabo de manera esporádica una operación con estos activos, su costo fiscal se determinará por el Artículo 75 del Estatuto Tributario, que le permite tomar *como costo presunto el 30 % del valor de la enajenación*. En todo caso, el ingreso será renta o ganancia ocasional, dependiendo de si el contribuyente lleva más de dos años con él [\[2112\]](#). Quien se dedique profesionalmente a comprar y vender criptoactivos, así como los mineros, la pérdida o ganancia por la fluctuación del valor del bitcoin en el mercado no debe ser reconocido por el contribuyente, *hasta tanto se realice la venta o enajenación del criptoactivo*, ya que el bitcoin no es reconocido como una divisa [\[2113\]](#).

Respecto del IVA, en Colombia se considera que están exentos los *Exchanges*, ya que no realizan el hecho generador. Respecto de los mineros, al igual que el licenciamiento de software tributa el IVA, se considera que los mineros deberían tributar el IVA igual que otras actividades informáticas, aunque el punto está muy discutido, ya que se afirma que no hay una prestación de servicios a un beneficiario determinado a quién facturar el servicio gravado [\[2114\]](#).

En Chile, a su turno, se ha afirmado [\[2115\]](#) que desde Junio de 2018 la tenencia de criptoactivos, considerados activos digitales inmateriales, pero no moneda de curso legal ni divisa, tributa Impuesto a la Renta al momento de su venta, y el valor de adquisición de dichos activos podrá deducirse como costo directo en la determinación de la señalada Renta Líquida Imponible. Con relación al IVA, el bitcoin, al igual que cualquier otro activo digital o virtual, carece de corporalidad y por ende no se encuentra alcanzada en el IVA la compra directa, entre usuarios [\[2116\]](#). También se ha considerado la tributación de los *Exchanges*, afirmándose que deben llevar contabilidad y

están alcanzados por el Impuesto a la Renta por su actividad habitual de intermediación, al igual que las *Wallets*, ya que cobran comisiones por sus servicios digitales, que son servicios de intermediación que además, están sujetos al IVA [\[2117\]](#). A la fecha en que se escriben estas líneas, en Chile no está claro cómo debe tributarse la venta de bienes o servicios pagados con criptomonedas, aunque la doctrina postula aplicar las mismas reglas tributarias que cuando se celebran contratos de permuta [\[2118\]](#), para lo cual las partes involucradas deben dejar constado el precio que le asignan a cada bien o servicio pagado con criptoactivos. Finalmente, respecto de la actividad de minería, se ha sostenido que en la determinación de la renta gravada, podrán deducirse gastos de electricidad, computadoras, accesorios y en general todo el hardware utilizado, así como contratos de alquiler, etc [\[2119\]](#).

5.4.3. La tributación de los criptoactivos en Argentina

Se ha sostenido [\[2120\]](#) que la Ley N° 27.430, en vigor desde el 1 de Enero de 2018, grava en el Impuesto a las Ganancias (IG) las rentas provenientes de las "monedas digitales". El término genera dudas entre los expertos porque tanto las UIF (Unidad de Información Financiera) como el FATF/GAFI e incluso la Unión Europea refieren a las criptomonedas como "monedas virtuales", por lo que algunos concluyen que en nuestro país lo que está gravado con el IG es algo más amplio que las criptomonedas. Estamos a la espera de que AFIP aclare qué entiende por "monedas digitales" y, en particular, si comprende a los tokens.

En virtud de la Ley N° 27.430, se incorporó un artículo a la ley del Impuesto a las Ganancias por el cual la ganancia que obtengan las personas humanas por la venta o transferencia de monedas digitales que estén ubicadas en el país y sean emitidas en pesos con cláusula de ajuste está gravada, como rentas de la segunda categoría –art. 45 inc. k), Ley del Impuesto a las Ganancias– a una tasa del 15% y cuando sean emitidas en pesos pero sin cláusula de ajuste la tasa es del 5%.

Se ha señalado que la ley fue redactada para otro tipo de bienes, como

acciones o títulos y eso la convierte en letra muerta para las criptomonedas. En primer lugar, las criptomonedas no se emiten en ninguna moneda -aunque coticen generalmente en dólares- y, en segundo lugar, las criptomonedas no se comercian en ningún país en particular dado que, en general, su transferencia se registra en la plataforma *blockchain* que está en cada nodo de acceso por lo que no puede decirse que las criptomonedas estén ubicadas en Argentina [\[2121\]](#). Sólo podría decirse que las criptomonedas están ubicadas en el país si se las deposita en una *billetera* domiciliada en Argentina pero, aunque en ese caso se pueda identificar la ubicación de la moneda, igualmente no puede decirse que la criptomoneda está emitida en determinada moneda.

Es por todo ello que en la práctica la norma específica no podrá aplicarse a las criptomonedas, lo que no quiere decir que las monedas digitales no estén gravadas de todos modos.

En efecto, cuando las monedas digitales estén depositadas en una billetera en Argentina la ganancia que se genere por su venta o transferencia está gravada sólo si el titular es *habitualista* en la compraventa de esas monedas. En ese caso, aplica la alícuota progresiva que puede ir desde el 5% al 35% de la ganancia. Si las monedas estuvieran depositadas en el exterior, la tasa del impuesto es fija y asciende al 15%, pero para estas monedas no se requiere ser habitualista por lo que cualquier persona que venda o transfiera monedas digitales en el exterior estará alcanzada por el impuesto aunque lo haga por única vez. En este sentido, y dado que cada impuesto cedular genera un quebranto específico, puede sostenerse que la pérdida o ganancia por tenencia y venta de criptoactivos puede compensarse contra la pérdida o ganancia devengada por el mismo tipo o categoría de activo, pero no por otra clase de activos [\[2122\]](#), y deberán compensarse rentas de fuente nacional contra quebrantos también de fuente nacional, y rentas de fuente extranjera, también contra quebrantos de fuente extranjera [\[2123\]](#).

Se ha afirmado que si una persona que vive en el país es titular de criptomonedas depositadas en una billetera electrónica en Argentina sólo abonará el Impuesto a las Ganancias por vender o comerciar con este tipo de

monedas *en forma habitual* ^[2124]. Si no negocia con esos valores habitualmente entonces el impuesto no resultará aplicable. Si esa misma persona es titular de criptomonedas depositadas en una billetera con domicilio en el exterior, la ganancia que obtenga por la venta de esas monedas estará gravada al 15%.

En el caso de los tokens, especialmente de los STOs y ICOs, la situación es distinta por varias razones. Los token operan de forma similar a un título valor porque otorgan al titular el derecho a recibir una participación en el capital o en los servicios que brindará determinado proyecto. Así, si AFIP los incluye en el concepto de "monedas digitales", les aplicarán los mismos comentarios que para las criptomonedas, y si no los incluye en ese término, podrían estar gravadas de igual forma que un título valor.

En el Impuesto sobre los Bienes Personales existe consenso respecto a que la tenencia de criptomonedas *está exenta por ser un bien inmaterial* ^[2125]. De esta forma, los titulares de criptomonedas no pagarán este impuesto por la parte de su activo que tengan en este tipo de monedas. Por último, las operaciones con criptomonedas tampoco están alcanzadas por el IVA ya que, al ser un bien inmaterial, no encuadra en ninguna de las operaciones que grava ese impuesto ^[2126]. Sin perjuicio de que las comisiones y cargos que se paguen por este tipo de operaciones sí estarán gravadas en el IVA ^[2127].

Finalmente, para el caso que se comiencen a desarrollar derivados sobre criptoactivos en Argentina, debe tenerse muy presente el fallo de 2017 de nuestro Máximo Tribunal, *in re Tecpetrol SA c/ DGI* ^[2128].

Allí, la actora pretendía que los quebrantos generados por ciertos contratos derivados fueran deducidos de su declaración de impuesto. La DGI se oponía, afirmando que la actora no puede compensar las pérdidas generadas por la utilización de los instrumentos o contratos derivados *que no son de cobertura* contra la ganancia neta del ejercicio fiscal en que se produjeron, sino sólo contra ganancias netas originadas en la utilización de este tipo de operatoria, que la DGI consideraba como *especulativa* y no de cobertura, ya que la actora no había demostrado el fin de cobertura subyacente a los contratos derivados

celebrados, y con los cuales intentaba cubrirse o mitigar el riesgo de su actividad consistente en hallarse expuesta a la volatilidad de los precios de comercialización del petróleo [\[2129\]](#). DGI afirmó incluso que justamente como existían pérdidas en esos contratos derivados, no habían funcionado como cobertura eficiente.

La Corte abordó directamente a los derivados. Analizó en primer término los contratos de futuros, afirmando que forman parte del género de los contratos derivados pues su valor depende o "deriva" de la valuación de ciertas variables subyacentes, sean estas activos financieros o activos no financieros, por ejemplo, las materias primas. Su concertación implica el compromiso de realizar una transacción sobre ciertos subyacentes ~ (en el caso, petróleo crudo), que se realizará en una fecha futura, a un precio que es determinado inicialmente por las partes, y cuya negociación se lleva a cabo mediante instrumentos estandarizados en un mercado formal que garantizará el cumplimiento del contrato (en autos, el mercado de New York NYMEX, en el que intervino como operador financiero la firma Merrill Lynch, Pierce, Fenner & Smith Inc.) [\[2130\]](#).

Puntualizó la Corte que una de las singularidades de esta clase de instrumento consiste en que diariamente, al finalizar las ruedas de negociación en aquel mercado, cada contrato tiene un precio de ajuste o precio de cierre que se utiliza para determinar los márgenes de variaciones producidas y, aun antes del vencimiento pactado en cada contrato, se pueden cancelar las posiciones tomadas originariamente -como parte vendedora o como parte compradora-, realizando una operación en sentido inverso a la inicial, con lo cual la operación se saldará mediante el pago o cobro en dinero de la diferencia existente entre el precio de compra y el de venta de ambos contratos, con la consiguiente pérdida o beneficio para cada parte. Esto es, la operación se resuelve sin necesidad de que se produzca la entrega física del activo.

Afirmó la Corte que a esta clase de operatoria se puede acudir con fines especulativos, cuando se apuesta a la evolución favorable en la variación de los precios de cualquier activo y solo se persigue la obtención de beneficios, o bien, con el propósito de cobertura, si su finalidad es reducir o suprimir un

riesgo inherente a la actividad que desarrolla una empresa y que esta evalúa como adverso [\[2131\]](#) .

Valorando la plataforma fáctica del caso, la Corte consideró que para la actora, el sentido de recurrir a una operación de cobertura consistiría en protegerse total o parcialmente de las posibles bajas que se produjeran -más allá de lo que aquella estima aceptable- en los precios de comercialización del petróleo crudo que se caracterizan por una alta volatilidad. Afirmó la Corte que no implica la inexistencia de pérdidas, sino que la actuación en ambos mercados -el mercado físico y el mercado de derivados- con la finalidad de cobertura busca neutralizar o "cubrir" el riesgo del siguiente modo: una pérdida en la venta pactada en el mercado de futuros -debido a que con posterioridad a su concertación se produce un alza de los precios- se compensará con el mejor precio que se obtenga al vender el producto en el mercado físico; a la inversa, la ganancia obtenida en el mercado de futuros -debido a que posteriormente a la celebración del contrato se produce una baja en los precios del activo subyacente- permitirá compensar el menor precio al que este será vendido en el mercado físico [\[2132\]](#) .

La Corte siguió con su estudio del caso, y analizó otro contrato derivado celebrado por la actora: concertó con la firma Margan Stanley Capital Group Inc varios contratos de "swaps" -contratos de canje o permuta de flujos de fondos- en los que las partes negocian la operación a realizar en un plazo futuro y a un precio fijado desde un inicio, sobre la base de la variabilidad de un activo subyacente, en el caso, cierta cantidad de barriles de petróleo crudo ("*swaps de commodities*"). Afirmó la Corte que el funcionamiento de la operatoria presenta rasgos similares a los futuros, pero puntualizó que a diferencia de éstos, los "swaps" se negocian en mercados no estandarizados ("Over The Counter"), y, si bien suponen la asunción de un riesgo mayor pues su cumplimiento no se halla garantizado, poseen una mayor flexibilidad en la negociación que le permite a las partes acordar a su medida todos los términos de aquel.

Muy sucitamente, en el caso de la actora, el sentido de acudir a esta operatoria con fines de cobertura consistiría en concertar mediante las operaciones de "swaps" la venta de cierta cantidad de barriles de petróleo

crudo a un precio fijado inicialmente y a una fecha futura en la que, por otra parte, deberá cumplir en el mercado físico sus compromisos comerciales de venta y entrega de aquel producto. En la fecha pactada en los contratos de "swaps", se liquidarán las diferencias resultantes entre el precio fijado en dichos contratos y el que resulte del precio internacional de mercado tomado como referencia, de manera tal que un alza de este último respecto del precio acordado en los "swaps", implicará para la actora la obligación de pagar el excedente o diferencia a su contraparte; por el contrario, de producirse una baja en la cotización, Tecpetrol S.A. recibiría de Margan Stanley Capital Group Inc., la diferencia entre esta última cotización y el precio establecido en los contratos de "swaps".

La Corte analizó, por último, que la actora ha concertado con la misma firma internacional otra clase de instrumentos derivados conocidos como operaciones "Zero Cost Collar", en las que, con el fin de acotar los riesgos de futuras fluctuaciones en el precio del petróleo crudo, se combinan dos contratos de opciones, fijándose una banda de precios limitada por un "piso" (precio mínimo) y un "techo" (precio máximo). Según la descripción realizada por la actora, si en la fecha futura que ha sido fijada al celebrar el contrato, "el precio real" del petróleo crudo se halla por debajo del "piso", Tecpetrol S.A. recibirá el cobro de la diferencia hasta alcanzar dicho "piso"; por el contrario, si el "precio real" se ubica por encima del "techo" fijado, la actora deberá pagar a Margan Stanley Capital Group Inc. esa diferencia y, finalmente, si el "precio real" se mantiene dentro de la franja de flotación establecida entre el "piso" y el "techo" no habrá cobros ni pagos para las partes.

Luego de valorar los contratos celebrados frente a la normas tributarias existentes a la época de los hechos imponible, la Corte rechazó el criterio de la AFIP, haciendo lugar al planteo de la actora y, en consecuencia, admitió que la ganancia del ejercicio se compense con las pérdidas devengadas por derivados de cobertura. Es de esperar que este criterio judicial sea extendido, a su turno, a los derivados de cobertura donde el subyacente son criptoactivos.

5.5. ¿Elaboración Participativa de Normas?

Habiendo pasado revista a cuáles fueron los primeros pasos hacia el entorno *blockchain* en Argentina; a cómo funcionan y cuáles son las instituciones de los mercados de dinero fiduciario y de capitales, valorándose las últimas innovaciones jurídicas en dichos ámbitos en relación a la digitalización de activos; a cuál ha sido el rol del BCRA, de la CNV y de la UIF; a la necesidad imperiosa de promover la digitalización de las Finanzas Sostenibles; y a los principales avances regulatorios que se registran en el Derecho Comparado de parte de reguladores con distintos poderes de policía, así como a la distinta forma de tributar que tienen los criptoactivos en el extranjero y en nuestro país, corresponde ahora cerrar este Capítulo V con algunas reflexiones sobre cómo avanzar con la regulación de este nuevo fenómeno jurídico-económico-tecnológico, hasta tanto exista una legislación que lo aborde holísticamente.

En este sentido, no debe olvidarse que cada vez que ha aparecido una nueva tecnología, los Abogados han tendido en general a tomar dos enfoques: (i) uno que favorece la coherencia, entendida como las normas, principios y categorías legales *precedentes*, y en donde el análisis gira en torno a cómo una nueva tecnología *encaja* en tales normas, principios y categorías *preexistentes*, con una lógica propia de un Juez o de un abogado litigante; y (ii) otro que favorece la llamada regulación *instrumental*, donde el análisis gira en torno a si las normas, principios y categorías legales precedentes *sirven o son eficientes* para regular una nueva tecnología, o si deben crearse nuevas normas, principios y categorías, con una lógica más propia de un Legislador [\[2133\]](#).

En general, los ingleses han sido siempre muy pragmáticos, y poco dogmáticos. Así, el enfoque de regulación *instrumental* inglés sobresale mundialmente, como un ejemplo de regulación práctica, que se ha manifestado principalmente en las acciones tomadas por la Financial Conduct Authority (FCA) y su mundialmente afamado modelo *SandBox*. Se afirma que Argentina haría bien en seguir el modelo inglés de regulación instrumental. Así, los reguladores –BCRA, CNV, etc.– debieran centrar el análisis en si las normas, principios y categorías legales precedentes *sirven o son eficientes* para regular una nueva tecnología, o si deben crearse nuevas normas, principios y categorías, con una lógica más propia de un Legislador.

Por ello, una forma interesante de abordar eficientemente este nuevo

fenómeno jurídico-económico-tecnológico, es a través de la generación de las nuevas reglamentaciones a través de procesos participativos de elaboración de normas, como ocurrió, por ejemplo, cuando CNV reglamentó las PFCs de acuerdo al mandato contenido en la LACE.

En este sentido, sin desconocer el carácter autárquico del BCRA, de CNV y de SSN, puede resultar conveniente aprehender el fenómeno *Fintech* argentino en general, y el entorno *blockchain* en particular, recurriendo al Reglamento General para la Elaboración Participativa de Normas aprobado por el Decreto 1172/2003, y empezar, paralelamente, a pensar en una ley que promueva genuinamente el crecimiento del sector *Fintech* argentino, entorno *blockchain* incluido, en el marco de la Economía del Conocimiento, sin poner en riesgo la solidez del sistema financiero y dando ciertas certezas a los *players*, a sus inversores, y especialmente escuchando al público general que utiliza sus servicios, los usuarios, tanto a las asociaciones de consumidores y usuarios como a las cámaras empresarias que representan a grandes usuarios.

El riesgo que percibo es que la ausencia de una clara definición legislativa a nivel nacional a favor de la innovación e inclusión financieras en general, y del entorno *blockchain* en particular, puede dejar abierta las vías para una regulación segmentada, asistemática y subsectorial por parte de BCRA, CNV y SSN, entes éstos que pueden ser permeables ante las presiones cada vez más fuertes de parte de los incumbentes [\[2134\]](#), que tienen un viejo conocido y poder de lobby, del cual carece el ecosistema *Fintech*. Sin dudas, el combate entre banca y *Fintechs* es asimétrico, y lo que está en juego es nada más y nada menos que la competencia, la innovación y la inclusión financiera, tres políticas de Estado que en Argentina deben ser potenciadas, y que debieran ser impulsadas con mano firme. No olvidemos el tristemente célebre Viernes 3 de Abril de 2020, cuando en plena pandemia del Covid-19, 800.000 jubilados y beneficiarios de ANSES fueron obligados a salir a la calle y hacer interminables colas para llegar a un cajero y obtener dinero físico, un *valor de curso legal* que puede, perfectamente, ser digitalizado y acreditado en una *Wallet* que opera desde cualquier Smart Phone con conectividad, y donde también se acreditan criptoactivos que, a no dudarlo, serán cada vez más populares. No olvidar el Yuan Digital...

En materia de regulación bancaria, no debe olvidarse que la banca

argentina sólo ha comenzado a innovar ante la insoportable presión generada por la rápida irrupción de las Fintechs [\[2135\]](#); es una banca que tiene un modelo de negocios centrado principalmente en asistir financieramente a un Estado con déficit crónico [\[2136\]](#), y se ha demostrado fehacientemente que tiende a no competir, a cartelizarse y a abusar de su posición: no olvidemos el tristemente célebre caso PRISMA [\[2137\]](#).

Cabe entonces preguntarse: ¿Serán las Fintech argentinas el gran disciplinador de un amañado y *poco competitivo* mercado de servicios bancarios y financieros, que tiene una muy pobre penetración, donde sólo el 50% de los adultos argentinos está adentro de la red bancaria [\[2138\]](#)? La banca ha logrado que los saldos disponibles de dinero electrónico de los clientes de PSPs deban *por defecto* ser depositados en cuentas bancarias, generando más comisiones bancarias (e impuestos) que terminarán pagando los usuarios de PSPs, como se vio en § 4.5.13.3. Es previsible que la banca presione, también, para que los *Exchanges* sean considerados PSPs, como se analizó en § 4.5.13.8.

VI. Casos de Uso en el Mundo de los Negocios. Smart Citizens

6.1. *Blockchains y Smart Contracts: Casos de uso en el Mundo de los Negocios.*

Habiéndose sintetizado en los cinco Capítulos precedentes las distintas nociones y apreciaciones de la *blockchain* y de los *Smart Contracts*, analizado los distintos enfoques legislativos y regulatorios así como los desafíos jurídicos que se plantean, corresponde ahora ilustrar al lector con casos interesantes de aplicación de estas tecnologías, tanto en el ámbito privado comercial como en el ámbito de los servicios públicos.

Algunas aclaraciones antes de seguir: (i) la que sigue no es una enumeración exhaustiva, sino más bien descriptiva de *algunos* ámbitos en que las tecnologías han sido exitosamente aplicadas, o están por serlo en el corto plazo; (ii) el único criterio seguido en la selección de casos descriptos ha sido el interés personal de la aplicación desde el punto de vista del autor; (iii) muchos de los ejemplos que se traerán a colación, no existirían si sus impulsores –*los Creadores de la Innovación*– hubieran aguardado el dictado de nuevas leyes, o la adaptación de las normas preexistentes; y (iv) muchos de los casos tratados demuestran un uso *instrumental* de la regulación, en el sentido de *crearse* nuevas normas y reglas para una nueva realidad, en lugar de aplicarse las preexistentes –temperamento absolutamente pro-innovación y pro-competencia.

6.1.1 *RegTech*

Quizás el caso más emblemático es Corda, analizado en § 3.2.2.1. También se inscriben en esta categoría las leyes dictadas en los Estados de Delaware, Illinois, Vermont y Wyoming, vistas en § 3.4.2.2.2. Recordemos que también apuntan al *RegTech* los Programas de Innovación Financiera que impulsa el BCRA, como se vio en § 5.1.

Un informe de Deloitte de Enero de 2020, identificaba 362 empresas

operando en el segmento *RegTech* en el mundo [\[2139\]](#), ofreciendo servicios de reporting, gestión de riesgos, control y gestión de identidad, *compliance*, y monitoreo de transacciones.

6.1.2. Energía

Empresas como PowerLedger [\[2140\]](#), WePower [\[2141\]](#) y EnerChain [\[2142\]](#) proponen decentralizar *on-chain* el mercado eléctrico minorista [\[2143\]](#).

WePower, desde Lituania, se presenta como *The easiest way to buy green energy directly from producers and reach your energy sustainability goals*, y opera un marketplace “that connects companies directly with green energy generators so that all companies can make a tangible environmental impact whilst buying green energy at competitive rates with full transparency”. Para lograrlo, utiliza Smart Contracts en Ethereum y apunta al mercado corporativo de consumo de energía eléctrica. PowerLedger, a su turno, tokeniza la energía producida mediante generación distribuida con paneles solares fotovoltaicos, y permite la reventa de dicha energía tokenizada en su plataforma, conectado compradores y vendedores. Su propuesta de valor es muy simple: “if you have solar panels on your rooftop you can use our platform to sell excess energy to your neighbor. If you have battery storage you can store your energy and sell it at the peak to maximize your profit from the solar power you generate. Similar to trading shares on a stock exchange you can set buy and sell prices so that you can trade energy at the right price for you. We give you security and peace of mind, by recording all transactions on the blockchain.” Esta empresa utiliza blockchain y Smart Contracts pero apuntando al mercado minorista.

EnerChain, por su parte, inició un piloto en 2017 y 2018, en el que participaron más de 40 utilities europeos. Apunta a crear una plataforma decentralizada de trading de energía *on-chain*, en estos términos:

“The Enerchain infrastructure can be used for wholesale products but also for those who create new decentralised

markets for highly innovative products – be it other commodities like coal and oil, PPAs, PoAs, or even other industrial products. Using a decentralised marketplace has not been technically and economically viable before the launch of Enerchain. Previously market participants traded products bilaterally in a less efficient way. The possibilities with the Enerchain are endless: over-the-counter trading, balance group management, wholesale trading and much more”.

Otros casos interesantes de aplicación de blockchain y Smart Contracts en el sector de la energía, son Grid+^[2144], Brooklyn MicroGrid^[2145], Greeneum^[2146], y Grid Singularity^[2147]. Es interesante ésta última, que tiene muchos casos reales de uso en Alemania^[2148].

6.1.3. Comercio Internacional

En Julio de 2019, el BID y el FORO ECONÓMICO MUNDIAL publicaron un White Paper titulado *Windows of Opportunity: Facilitating Trade with Blockchain Technology*^[2149]. En el documento se afirma que:

“blockchain can help diverse stakeholders interoperate by enabling them to access the same data at the same time (hence the term “distributed ledger”); Smart Contracts built on a blockchain can automate stakeholders’ compliance with various contractual obligations; and blockchain data is a stream of reliable information on past transactions as they are immutable once entered”^[2150]

Si bien desde el BID y el FORO ECONÓMICO MUNDIAL se promueve el uso de la *blockchain* en materia aduanera vinculada al comercio internacional

como elemento *RegTech*, también se afirma que:

“What can be said is that **blockchain is not a silver bullet that cures all ills in world trade** –what it can and cannot do well can be defined only through further testing and piloting. Many governments that have been successful in automating their border processes – such as the United Kingdom, Korea, Singapore, Mexico and the United States – are today the most avid experimenters with blockchain in customs and single windows, precisely to assess the technology’s potential in offering new efficiencies and capabilities. **Also, many leading logistics companies and banks are exploring blockchain for streamlining their operations.**” (el resaltado es mío).

Notablemente, señalan desde el BID y el FORO ECONÓMICO MUNDIAL un piloto en *blockchain*, conocido como CADENA, al que describen como:

“During 2018, the IDB, together with the customs administrations of Mexico, Peru, Costa Rica and Chile, and with technical support from Microsoft, designed a solution using blockchain technology called CADENA v.0.33. It facilitates the sharing of the data associated with Authorized Economic Operator (AEO) certificates among customs administrations as specified in their mutual recognition agreements (MRA). While AEO programmes enable companies to facilitate their trade and save time and money in their trade transactions, CADENA helps to secure and facilitate supply chains globally. CADENA has been designed, first, to find a solution to a customs and border management challenge – the sharing of cross-border data – and secondly, to enable customs to learn about blockchain in order to consider possible further use-cases. Blockchain enables different national customs authorities to access the same verified, tamper-proof and real-time data. This ensures that traders can receive MRA benefits both at the countries of origin and destination of their

exports as soon as they are granted their AEO certification. During the pilot project, customs validated the benefits of the technology for sharing cross-border data, providing timely information about the level of compliance of traders to feed risk-management systems. Furthermore, they found that CADENA could next be expanded to automate the entire AEO certification process, and to other customs functionalities that require engagement with different stakeholders, both public and private. To build on the findings made during CADENA and to incorporate new developments in blockchain technology in 2018, a new phase is proposed to develop CADENA v.1 during 2019. CADENA v.1 will scale to other countries, such as Colombia, and will benefit from the synergies of LACChain (see Box 5) to address further issues related to governance, administration, data privacy, sustainability and scalability.”^[2151] (el resaltado es mío).

Apuntando también a facilitar el comercio internacional, *TradeLens*^[2152] es una plataforma en *blockchain* desarrollada por IBM y Maersk, que procura digitalizar el proceso de la logística y comercio marítimo.

Su propuesta de valor es contundente y muy exitosa:

“shippers can gain access to the breadth of an ecosystem which spans the **entire global logistics industry from customs authorities and agents to international and regional carriers**. The flow of reliable, trustworthy information plus the TradeLens platform’s ability to address core pain points through digitization and the replacement of paper-based processes is helping drive an industry-wide transformation. More than **\$16 trillion USD worth of goods are shipped across international borders each year**, with some 80 percent transported by the ocean shipping industry where SPIL play its role. **Paper-based procedures cause a number of pain points**

felt throughout the global supply chain, including inconsistent and inaccurate information, delays and disruptions (due to manual checking and data input), the inability to provide thorough risk assessments, the promotion of complex, inefficient and costly stakeholder communication, and a lack of transparency. The scope of the TradeLens platform now extends to **more than half of the world's ocean container cargo and the ecosystem now includes more than 160 participants**. It is commercially available and open APIs are public and can be openly accessed. TradeLens is an open and neutral industry platform underpinned by blockchain technology, supported by major players across the global shipping industry. The platform promotes the efficient, transparent and secure exchange of information in order to foster greater collaboration and trust across the global supply chain. [\[2153\]](#)” (el resaltado es mío).

También merecen resaltarse los avances en materia de *blockchain* y crédito documentario [\[2154\]](#), toda vez que una es posible programar *Smart Contracts* que vinculen al importador y al exportador, para garantizar el pago de una letra de cambio, emitida en *blockchain*, y vinculando a los bancos que intervienen en esta operación típica del comercio internacional. Esto permite que:

“Letter of Credit’s requirements are documented in a Smart Contract which exactness and precision on the contractual conditions like time and place of delivery, mode of delivery and quality of the product. It allows for more transparency around transactions and operations, including everything from tracking invoices to digitizing documents. **The issuing bank can verify condition on the basis of documented submitted by exporter/advising bank effectively removing ambiguity. All stakeholders have visibility of the latest state and any discrepancies can be resolved faster.** Any change/amendment

can be processed faster and in cost-effective way through a multi-signatory mechanism.”^[2155] (el resaltado es mío).

En este sentido, el banco HSBC ha desarrollado una plataforma propia en *blockchain*, llamada *Contour*, lanzada en Singapur^[2156] y en la que participan cincuenta bancos y empresas globales de catorce países. La idea: muy sencilla, migrar a la *blockchain* todos los procesos bancarios que tienen lugar en una carta de crédito:

“by digitizing the process, Contour has reduced the time taken from 5-10 days to as little as 24 hours. The group ran a survey, and 86% said traditional LoCs were too reliant on paperwork, and the process is becoming ‘intolerable’ for both corporates and Banks (...) “Clients have clearly seen the value of blockchain technology to digitise Letters of Credit. Besides reducing friction, it helps accelerate the velocity of trade, while allowing them to control their own data.” The backers of the project are Bangkok Bank, BNP Paribas, CTBC, HSBC, ING Bank, Standard Chartered, SEB, consultants Bain & Company and technology partner CryptoBLK as well as R3 (...) Like many blockchain projects, the launch is relatively ‘soft’. So no banks are live or in production yet, and the network is in beta stage. However, the company has been incorporated in Singapore, which is a feat in itself. The contracts for these sorts of ventures sometimes exceed more than a hundred pages. The project is based on R3’s Corda distributed ledger technology (DLT) (...)“The opportunity cost in trade finance is huge. Trillions of dollars in commodities, products and services are transacted daily, but the sector is still characterised by slow, duplicative and expensive processes.”^[2157] (el resaltado es mío).

Casos actuales de uso de la *blockchain* y los *Smart Contracts* son, por ejemplo, una exportación de algodón de EE.UU a China:

“A case study on a cotton supply chain proof of concept in which 88 bales of cotton were shipped from the US to China illustrates how Smart Contracts work in practice. The participants claim that **this was the first global trade transaction between two independent banks that combines the emerging disruptive technologies of blockchain, Smart Contracts, and Internet of Things (IoT), for a real transaction and shipment of goods.**”^[2158] (el resaltado es mío).

6.1.4 Industria automotriz

Existen ya varios casos de uso de *blockchain* en la industria automotriz. BMW en 2019 se unió a VeChain^[2159], y desarrollaron una aplicación en *blockchain* llamada *VerifyCar*^[2160]:

“The BMWs are equipped with various sensors that record every interaction with the vehicle, which is then stored with a hash key in the blockchain. The type of data stored can be anything from **changing the battery, replacing a filter, having the annual service, the odometer data**, etc. Each car has a SIM card that sends out datasets on a regular basis, which are then **verified and stored on the VeChain blockchain** (...) “What we tried to do here is to build a **digital passport that verifies datasets and allows people to know if what a seller says is really true.**” One solution they’re aiming to provide is ensuring that when a vehicle owner goes to resell their BMW, **the vehicle’s complete history is transparent and available to the buyer.** In Germany, it’s estimated that 33% of second-hand cars have manipulated odometer readings, equating an average economic impact of 3,000 EUR per car (...) VerifyApp and

VeChain blockchain have already been tested with internal vehicles and are ready for launch.” (el resaltado es mío).

Respecto a las funcionalidades de VerifyCar, se ha sostenido que

“The automobile industry has been the victim of fraudulent practices for decades. Odometer fraud, falsified vehicle repair history, dealership fraud and other **data manipulation** is becoming more common with each passing year. To combat this, BMW and VeChain have been working together to develop an immutable blockchain vehicle passport system that works in unison with their new mobile application VerifyCar. **At this time, insurance providers, repair shops, banks and other constituents store data on their own databases meaning there is no single source of truth. By storing all the data on an immutable distributed ledger, each party is able to access transparent information about the vehicle instantly, making the entire process simpler and more efficient.** VerifyCar connects BMW’s datasets directly to the VeChainThor Blockchain and **documents the entire maintenance and repair history of the vehicle. Additionally, the system keeps track of ownership transfer records, mileage, vehicle health and other data in real-time. It also utilizes Internet of Things technology and is combined with a unique VeChain ID that is given to each vehicle (...)** The VeChainThor Blockchain is a perfect tool to help streamline the manufacturing and distribution process of the supply chain management system. BMW, like most automobile manufacturers, has production plants located on several continents across the globe. **The supply chain must be able to pinpoint the shortest and most efficient shipping distribution routes to send vehicles and vehicle parts from one location to another.** These large distances come with immense challenges that make it essential to be able to link

manufacturing plants and distribution channels together. Throughout this process, **the blockchain tracks the location of vehicles and vehicle parts in real-time.** This drastically increases efficiency and reduces costs, making the supply chain system faster and more reliable (...) **When a stolen automobile is connected to the blockchain it is very difficult to sell the vehicle because of the traceability features that the technology provides. Blockchain technology could one day make it impossible to steal a car even if thieves are using the most advanced practices available.** By utilizing VerifyCar it will become nearly impossible for thieves to get away from law enforcement after a vehicle is stolen because the present location of the vehicle is tracked at all times (...) Blockchain technology could act as a major deterrent to car thieves by **offering verifiable and unchangeable vehicle titles.** Data regarding vehicles including ownership, insurance events, technical details, and more, could be written in to a Blockchain making the entire history of a vehicle traceable. This protects data important to the buyer and prevents thieves from being able to forge data belonging to the title (...) BMW has **existing systems in place such as DriveNow, ParkNow and ChargeNow in order to make it easier for owners to charge, park and share their vehicles** using a similar business model to Uber. VeChain's blockchain technology could help **enhance these technologies so it could soon be possible for a vehicle to drive, park and charge itself.** Payments for specific tasks such as parking could also be enabled by using machine to machine communication, blockchain and Internet of Things technology in unison. VeChain's blockchain technology could even be used to construct entire robot-controlled taxi fleets to pick customers in exact locations at a specific time. Autonomous driving is advancing so quickly that soon this technology could be much safer than human-driven vehicles. Blockchain will surely help make this vision a reality as society continues to move into the future.” (el resaltado es mío).

BMW sin dudas lidera la implementación de *blockchain* en su modelo de negocios. En efecto:

“the luxury automaker currently has a pilot program with suppliers with plants in Europe, Mexico and the U.S. and is using blockchain to track materials, components and parts across its supply chain. BMW is also a member of the Mobile Open Blockchain Initiative (MOBI), which is made up of a consortium of auto manufacturers including Honda and Ford. In July 2019, Mobi launched the auto industry’s first blockchain vehicle identity standard, which gives new cars a digital identity. The technology could eventually track events throughout a car’s life and be used to connect vehicles to share information, track speed, location, direction of travel, braking and even driver intention (like changing lanes).”^[2161] (el resaltado es mío).

Daimler, por su parte, también está aplicando *blockchain* en su cadena de suministros, con foco en la sustentabilidad:

“The project partners use blockchain technology to track the emissions of climate-relevant gases as well as the amount of secondary material along the complex supply chains of battery cell manufacturers. In addition, the data network documents whether the Daimler sustainability standards are passed on throughout the entire supply chain.”^[2162]

Toyota, por su parte, no se quiere quedar atrás. En Marzo de 2020^[2163], y en el marco del Toyota *Blockchain* Lab creado en 2019, Toyota anunció que planea incorporar *blockchain* para su negocio en varios ámbitos. Se afirma:

“In an era when all things and services will be connected by

information, blockchain is expected to be a fundamental technology that supports connecting people and businesses more "openly," in a manner that provides safety and security. In this regard, Toyota Blockchain Lab will expand collaborations more than ever with various partner companies. The progress of the IoT has connected various things and services through information and brought greater convenience and efficiency. On the other hand, it has increased the importance of responding to security concerns such as information leakage, tampering, and unauthorized use. In the automotive industry, during a once-in-a century period of profound transformation, Toyota is aiming to become a "Mobility Company" that provides wide-ranging services related to transportation. In realizing this goal, to promote "making friends" both inside and outside of the Group, it is important to create an environment where customers who use products and services and various businesses that provide them can connect more "openly" under "safety and security." With features such as highly tamper-resistant and fault-resistant, **blockchain technology can realize secure data sharing between various parties by improving the reliability of the information.** This technology has the potential to support the creation of friends inside and outside the Group, and as a result, provides more convenient and customized services to customers, business efficiency and improvement, and creating new value that is not bound by existing concepts.

To pursue the possibilities of this blockchain technology and gather momentum for initiatives, a virtual organization, Toyota Blockchain Lab, was established in April 2019 as a company comprised of six Group companies. As the spark for utilization of the technology, Toyota Blockchain Lab has been examining plans for promising applications for use and promoting demonstration trials while accumulating Group knowledge. It is also engaging in global collaboration with Group companies, including Toyota Research Institute - Advanced Development, Inc. (TRI-AD), TOYOTA Connected Corporation, and Toyota

Motor North America, Inc., and relationship-building with partner companies. In the following initiatives focused on customers and vehicles, demonstration trials under specific conditions were completed in November last year, confirming the usefulness of blockchain technology in each use application.

Customers - increasing convenience through ID sharing and contract digitalization inside and outside of the Group, improvement of personal information management, and utilization of points services

Vehicles - improvement of various services and creating new services through accumulation and use of all information concerning vehicle life cycles

Supply chain - improving business processes efficiency and traceability by recording and sharing information on parts manufacturing, shipping, etc.

Value digitalization - utilization for diversification of financing methods through the digitalization of various assets such as vehicles and various rights, and by that means, building medium to long term relationships with customers and investors.” [\[2164\]](#) (el resaltado es mío).

6.1.5. *Industria aeronáutica*

Honeywell, fabricante de motores de avión, ha desarrollado una plataforma en *blockchain*, llamada *GoDirect Trade* [\[2165\]](#), que opera como un marketplace de partes de aeronaves usadas:

“Honeywell’s GoDirect Trade platform collects information about aircraft parts over their entire life cycle and makes it available to potential buyers prior to the sale. Using a blockchain ledger allows Honeywell to securely aggregate this information from multiple, often competing, players. In its first year, GoDirect Trade processed more than \$5 million in online

transactions.”^[2166]

6.1.6. Mercados bancarios y financieros

Evidentemente, el ámbito de las finanzas ha sido, es y será muy fértil en materia de aplicación de *blockchain* y *Smart Contracts*. Veamos algunas aplicaciones actuales.

El caso de *Finality*, adelantado en § 5.2.3.3.3.7 es uno de los más relevantes, ya que participan en él los principales bancos del mundo^[2167]. *Finality* será lanzada en 2020^[2168] para servir como moneda de pago inter-bancaria y mayorista llamada *USC*, *utility settlement coin*, y fue creada para:

“to create a network of decentralised Financial Market Infrastructures (dFMIs) to **deliver the means of payment-on-chain in tomorrow’s wholesale banking markets**. *Finality*, backed by a consortium of Financial Institutions, including many of the Globally Systemically Important Banks (GSIBs), who sponsored the '**USC Project**' believe that **there will be widespread adoption of tokenisation, both for new and for existing assets**, creating new Value Chains. **A means of payment is an essential need for those Value Chains**. The shareholders of *Finality* comprise: Banco Santander, Bank of New York Mellon, Barclays, CIBC, Commerzbank, Credit Suisse, ING, KBC Group, Lloyds Banking Group, Mizuho Bank, MUFG Group, Nasdaq, Sumitomo Mitsui Banking Corporation, State Street Bank & Trust, and UBS.” (el resaltado es mío).

Finality propone desarrollar:

“a new payment system that will enable tokenised, peer-to-peer markets. *Finality* Global Payments (FGP) will comprise a series

of national systems, each regulated in its home jurisdiction. We call each of these a Finality Payment System (FPS) In each payment system, **USC will act as the settlement/payment asset for any Payment (P), Delivery v, Payment (DvP) or payment vs. payment (PvP) need.** [\[2169\]](#) **It's a pre-paid system:** for Finality users, Global Payments will fund their account in any currency available at that moment – funds which can be taken out at any time – and **for every unit of USC in circulation, there's a corresponding amount of collateral in that fiat currency.** “So, if there's a billion pounds’ worth of USC in circulation, there's a billion pounds at the Bank of England.” [\[2170\]](#) (el resaltado es mío).

Por otro lado, Bancos líderes como el JPMorgan vienen desarrollando distintos usos de *blockchain*, a través de una *blockchain* propia y de desarrollo interno, llamada Juno, en 2015 [\[2171\]](#). Simultáneamente, desarrolló otra *blockchain* propia, Quorum, que corre en Ethereum [\[2172\]](#). Finalmente, en 2019 se anunció la JPMorgan *Coin*, un StableCoin propia, atada al Dólar, que permite cambiar Dólares por esta criptomoneda, a los clientes del banco. Fue el primer banco norteamericano en lanzar su propia criptomoneda, pensada para clientes institucionales del banco [\[2173\]](#). Se ha sostenido que:

“JPM Coin is not money in the ordinary sense. Instead, it is a **digital token that represents U.S. dollars held by JPMorgan Chase.** It maintains a value equal to one U.S. dollar (...) It will be relatively straightforward for clients to use JPM Coin. First, **a client deposits a sum in a particular account and receives corresponding JPM Coins.** Next, these coins can be used to facilitate transactions across a blockchain network and with other JPMorgan clients. Finally, clients may redeem their JPM Coins with the bank to receive U.S. dollars at any time. While JPM Coin is similar to other stablecoins, there are also some

crucial differences. First, most stablecoins are open access and available to the public. On the other hand, JPM Coin will only be available to specific JPMorgan clients with proper permissions. In particular, those **clients must be institutional customers of the bank. JPM Coin is designed to facilitate the transfer of funds**, while most stablecoins are seen as investment tools. Finally, JPM Coin will always be redeemable in fiat currency held by JPMorgan. That makes it much more transparent than many stablecoins, such as Tether.”^[2174] (el resaltado es mío).

También se ha comentado antes, en § 4.5.11 sobre *Bakkt*, al empresa de *blockchain* lanzada por los controlantes del NYSE, *Intercontinental Exchange* (ICE), y que ofrece contratos derivados para criptoactivos que permitirán cubrirse del riesgo de volatilidad mediante contratos de futuros y opciones, con licencia de la CFTC^[2175].

Bakkt ya recibió más de 1.000 millones de Dólares de inversión, de inversores como Microsoft y Boston Consulting Group^[2176], con lo cual, es un nuevo Unicornio. Bakkt apunta a:

“By combining Bakkt’s enterprise-grade bitcoin custody offering with Intercontinental Exchange’s federally regulated futures exchange and clearinghouse, the **Bakkt Bitcoin Futures and Options contracts offer a fully regulated marketplace for the price discovery of bitcoin**. These contracts help support the hedging and risk management requirements for a broad range of institutional market participants.”^[2177] (el resaltado es mío).

La *blockchain* y los *Smart Contracts* también se están utilizando en préstamos sindicados. Los préstamos sindicados están indirectamente reconocidos y regulados en el art. 142 de la Ley de Financiamiento Productivo

Nº 27.440 en estos términos:

“Art. 142.- I. Agente de garantía. En los contratos de financiamientos con dos (2) o más acreedores, las partes podrán acordar la constitución de garantías hipotecarias y prendarias a favor de un (1) agente de la garantía, quien actuará en beneficio de los acreedores y a prorrata de sus créditos, de conformidad con las facultades y modalidades que se establezcan en los documentos de financiamiento y según las instrucciones que le impartan los beneficiarios de la garantía. En tal supuesto, los créditos asegurados por la garantía podrán transferirse a terceros, quienes serán beneficiarios de la garantía en los mismos términos que el cedente, no siendo de aplicación lo previsto en el artículo 2.186 del Código Civil y Comercial de la Nación.

II. Oponibilidad. En el caso de garantías prendarias o de otro tipo, sean fiduciarias o no, sobre créditos presentes y futuros del giro comercial del deudor o un garante, a los efectos de la oponibilidad frente a terceros en los términos del artículo 1.620 del Código Civil y Comercial de la Nación, será suficiente la publicación por la parte prendante de un aviso de cesión en el diario de publicaciones legales de la jurisdicción de la sociedad y en uno de los diarios de mayor circulación general a nivel nacional dando cuenta del otorgamiento de la garantía o la cesión en prenda al agente de la garantía de los créditos presentes y futuros, sin que sea necesaria, a tales efectos, la notificación específica al deudor cedido.”

Synaps [\[2178\]](#) es una empresa que ofrece una plataforma en *blockchain* y *Smart Contracts* para la gestión inteligente de préstamos sindicados bancarios. El primer piloto de la *blockchain* tuvo lugar en 2017 junto con R3 – los creadores de Corda–, con la participación de 19 bancos [\[2179\]](#). Capgemini es otra empresa que ofrece soluciones en *blockchain* para préstamos bancarios

sindicados [\[2180\]](#).

R3, los creadores de Corda, también han desarrollado una plataforma en *blockchain* llamada *MarcoPolo* [\[2181\]](#), que apunta, nada más y nada menos, a digitalizar las cadenas de suministro y el comercio internacional con un enfoque *RegTech*, y en la cual ya participan 28 instituciones, entre ellas los bancos líderes. MarcoPolo se presenta como:

“The Marco Polo Network is the largest and fastest growing trade and working capital finance network in the world. It is a joint undertaking between technology firms TradeIX and R3, the world’s leading financial institutions, and their corporate clients. The Marco Polo Network provides an open enterprise software platform for trade and working capital finance to banks and corporates and a distributed, blockchain-powered solution that allows for the seamless and secure exchange of data and assets between participants. Its mandate is to provide a dramatically improved customer experience using cutting-edge trade and working capital procedures, to enable seamless data integration and exchange between trading parties. Marco Polo aims to gather together the entire trade ecosystem. **It is a network at its core, uniquely positioned to enable its members to benefit from “network effects”.** In other words, every time a new organisation joins, the value of the Marco Polo Network increases for every other participant.” [\[2182\]](#) (el resaltado es mío).

En 2018, el banco BBVA y dos bancos más implementaron exitosamente en *blockchain* el primer préstamo sindicado del mundo [\[2183\]](#) con Red Eléctrica Corporación:

“Each step of the negotiation leading to the signing of the final agreement is recorded in the DLT network along with a **user**

code and the timestamp that identifies the moment at which the event occurred. Thus, all nodes participating in the private blockchain network (Hyperledger) **have access and share the same relevant information** of the negotiation process, and thus can stay informed of the status thereof, guaranteeing the **immutability of the information**. Finally, once the contract is signed, a unique document identifier is recorded in Ethereum's public blockchain network (specifically, in its test network, 'testnet') to guarantee its immutability against third parties while safeguarding its confidentiality at all times.” (el resaltado es mío).

En 2019, el banco BBVA ganó el premio a la innovación sectorial otorgado por la organización inglesa The Banker ^[2184]. BBVA ofrece servicios de *Do It Yourself* combinando *blockchain* y *Smart Contracts*, permitiendo a clientes institucionales y del sector público diseñar a medida su bono o su préstamo, on-chain y utilizando *Smart Contracts*:

“that BBVA **combines private and public platforms**: the private platform, based on Hyperledger, allows the whole process to be perfectly monitored and traced by all parties involved; and the use of a public hash recorded in the public blockchain Ethereum with a time-stamp that validates and ensures the immutability of the agreement. “The project has changed the way corporate clients interact with BBVA, thanks to a process that increases transparency” through the use of **Smart Contracts, which guarantee that the process remains simple and all related information stored in an immutable ledger, explains the publication**. The fact that BBVA encourages **clients to host their own blockchain nodes** and that it is building a **do-it-yourself portal** for this type of transactions are seen as key traits that set BBVA's proposal ahead of the pack. ‘The Banker’ also notes that BBVA has tested its platform with different financial instruments,

including **corporate loans, syndicated loans and structured bonds**, with deals ranging from €35 million to €1 billion.”^[2185] (el resaltado es mío).

En Abril de 2019, para la Comunidad de Madrid, el BBVA estructuró un préstamo verde por 220 millones de Euros, negociado y estructurado íntegramente en *blockchain*^[2186]. La operación fue un *Schuldscheine*^[2187], un tipo de préstamo a mediano plazo muy utilizado en Alemania, que se coloca de manera privada y que no está garantizado. Se documenta mediante un contrato de préstamo y un certificado de deuda que hace referencia al préstamo. No se trata de un título valor con oferta pública, y de hecho no cotizan en ningún mercado ni tienen ningún tipo de garantía. Normalmente, un banco negocia la operación con el deudor, coloca el préstamo y luego vende la partes en la participación del préstamo a otros bancos e inversores institucionales, mediante cesión de derechos o cesión de posición contractual en el préstamo subyacente, cesiones que son aceptadas de manera anticipada por el deudor. En esta operación, 100% digitalizada en *blockchain*, cada parte es un nodo, con acceso a todo los documentos digitalizados, y cada paso del proceso puede ser visto por todos los actores de la red privada, y queda un *hash* en Ethereum pública^[2188].

También en 2019, Wave Financial^[2189], una empresa de inversiones especializada en activos digitales y tokenizaciones, lanzó un fondo de inversión que opera con derivados en Bitcoin, vendiendo opciones de compra de bitcoins^[2190]. Las cuotapartes del fondo están tokenizadas:

“Wave BTC Income & Growth Digital Fund will issue **Fund Tokens** based on cryptographic technologies similar to those used for creation and transfer of select virtual currencies. Wave anticipates that Tokens will be able to be traded on alternative trading systems at a later date. An investment in Fund/Tokens is suitable only for sophisticated investors who have experience investing in private funds employing the Fund's strategies, are

familiar with investing in and trading Crypto Assets and can afford the loss of their entire investment in Fund/Tokens. **The Fund will sell Fund/Tokens only outside the United States to non-US persons in compliance with Regulation S under the Securities Act of 1933 or, within the United States, only to "accredited investors" within the meaning of Rule 501(a) of Regulation D under the Securities Act, pursuant to an exemption from registration provided by Rule 506(c) of Regulation D.** The Fund/Tokens are only available for purchase through the Fund or broker/dealers engaged by Wave on behalf of the Fund. The offer and sale of the Fund Tokens, the Fund, and its managers are not and will not be registered with the Securities and Exchange Commission, and are not subject to disclosure and certain other requirements mandated by U.S. federal securities laws, and investors therefore will not benefit from the protection of such laws.” (el resaltado es mío).

Wave Financiam también opera en el mercado de tokenizaciones, habiendo por ejemplo tokenizado 25.000 barriles de Whisky de Kentucky, que serán vendidos en un período de 6 años, con una rentabilidad esperada del 20% [\[2191\]](#). También deben recordarse los casos de *SDX* y *Linq*, vistos *supra* en § 3.3.2.2.

6.1.7. Real Estate

Un informe de Deloitte de Marzo de 2020 [\[2192\]](#) indica que *blockchain* comienza a ser muy utilizada en el *commercial real estate*. Señala Deloitte los beneficios de utilizar *blockchain* en los negocios inmobiliarios:

Imagen 14 Deloitte

Why consider blockchain for real estate leasing and purchase and sale transactions?



Need for a common database

Shared databases are critical for leasing and purchase and sale transactions. One of the key examples is a multiple listing service, which collates property-level information from private databases of brokers and agents.



Multiple entities can modify database

Transacting and managing real estate properties involves several entities, such as owners, tenants, operators, lenders, investors, and service providers, who provide, access, and modify a variety of information.



Lack of trust among entities

Many times, participants in leasing and purchase and sale transactions are new to each other and could be over cautious in due diligence and may even have data integrity concerns. However, blockchain can help reduce the risk through digital identities and more transparent record keeping systems for real estate titles, entitlement, liens, financing and tenancy.



Opportunity for disintermediation

Trusted intermediaries such as title companies can be disintermediated through blockchain, due to increased security and transparency in title management and auto-confirmation by government land registries.



Transaction dependence

Many real estate transactions have conditional clauses and can be executed through smart contracts. For instance, the conclusion of a purchase-sale transaction could be dependent on loan approvals or title clearances.

Source: Gideon Greenspan. "Avoiding the Pointless Blockchain Project," LinkedIn, November 24, 2015; Deloitte Center for Financial Services analysis.

Se firma que la *blockchain* puede ser utilizada en cinco procesos propios del sector: (i) anuncio de propiedades en alquiler a través de plataformas públicas de *blockchain*; (ii) due diligence pre-contractual, utilizando identidades digitales para los inquilinos y para las propiedades, de modo de conocer rápidamente los gravámenes que afectan a una propiedad; (iii) digitalización de contratos de alquiler y leasing mediante *Smart Contracts*; con pagos automatizados con criptoactivos; (iv) creación de garantías inteligentes a

través de *Smart Contracts* que aseguran el cumplimiento de las obligaciones contractuales asumidas; y (v) on-chain data analytics [\[2193\]](#).

Con relación a la compra y venta de propiedades, el proceso también puede ser digitalizado en *blockchain*, a medida que los títulos dominiales, autorizaciones administrativas, permisos de edificación, sean volcados a la *blockchain*. Esto permitirá, más cerca que lejos, programar *Smart Contracts* y smart mortgages sobre una propiedad, con pagos en criptoactivos o en dinero fiduciario, interconectados con los registros públicos, que tendrán acceso en tiempo real a los cambios dominiales ocurridos, y a las garantías constituidas. Afirman desde Deloitte:

“Commercial Real Estate market participants should consider **developing digital identities for a property** to keep pace with the growing preference for digital transactions. As the name suggests, digital identity with respect to a real estate property would imply **a digital identifier that consolidates information such as vacancy, tenant profile, financial and legal status, and performance metrics in digital form**. A combination of blockchain technology along with digital identity can alleviate the above-discussed challenges of physical identity proofs, and expedite a few of the pre-transaction activities such as underwriting, financial evaluation, obtaining a mortgage commitment, etc. An August 2016 Deloitte-World Economic Forum report titled “A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity” mentions that a “digital identity would allow financial institutions to perform critical activities with increased accuracy over that afforded by physical identity, and to streamline and partially or fully automate many processes.” Having said that, data integrity is critical for accurate digital identities and blockchain transactions. **The reality is that the initial data would be as good as the user entries**. To ensure accuracy, different participants such as tenants, investors, financing sources and advisors, etc. could validate the data. In fact, if companies

experimenting with blockchain technology also consider using the digital identity of property and people, the result can have a powerful impact on reducing the current inefficiencies and inaccuracies. **Digital identities of properties linked to the digital identities of transacting parties can create valuable and secure online records for a property, improve lease information management, and greatly ease the due diligence process.**^[2194] (el resaltado es mío).

Con relación al uso de *Smart Contracts* en negocios inmobiliarios, se afirma:

“Executing a real estate lease using Smart Contracts can address many of the challenges associated with property and cash flow management. According to Nick Szabo, a prominent thought leader of blockchain and Smart Contracts, “a Smart Contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.” **For the real estate sector, the traditional lease contract can morph into a smart tenancy contract. The use of a smart tenancy contract on a blockchain platform would enable transparency in lease terms and transactions. The contract could use rent or bonds for automated payments to real estate owners, property managers, and other stakeholders along with near real-time reconciliation.**^[2195] (el resaltado es mío).

Empresas que ya están encarando este desafío del *blockchain* y real estate son, por ejemplo, Atlant.io^[2196], dedicada a la tokenización inmobiliaria. Ofrece una plataforma en la que los vendedores de inmuebles pueden tokenizarlos para comercializarlos a través de token sales a inversores que los adquieren, i.e., adquieren una porción del precio a pagar, o del contrato de alquiler del inmueble, o ambas cosas.

Midasium^[2197], por su parte, ofrece una *blockchain* que articula con

Smart Contracts, en la cual se registran:

“By creating a global ecosystem for residential and commercial property where transactional and registry functions can be tracked in real-time: (i) Land titles and mortgage registrations (ii) Tenancy and bond arrangements. **The ecosystem will create the world's first Virtual Credit Bureau for real estate.** Giving property and financial service providers a more up to date and standardised view of property and credit metrics. The foundation of the bureau will be built upon a global decentralised ledger for real estate called the Midasium Blockchain. **The purpose of the blockchain is to execute and retain a permanent history of all real estate transactions and registrations using a system of Smart Contracts known as Midasium Contracts.** The Smart Contracts replace traditional contracts such as: Mortgage agreements, Contracts of sale and Tenancy agreements. What makes Midasium Smart Contracts advantageous over traditional contracts are that they remove various human elements and legacy technology in today's current processes. The result is: (i) a near instantaneous settlement time; (ii) a reduction in legal, accounting and transaction costs; (iii) and a significant reduction in fraud, corruption and credit risk. The Midasium Blockchain does this by storing contracts and related metrics in such a way, that **when granted permission, a full financial history of a property can be traced and audited.** With this, financial benchmarks can be easily obtained such as property defaults and vacancy rates. Using advanced cryptography, **confidential information is securely encrypted from public view. Only contract signatories can grant permission to third parties in order to view the details.** However, signatories may be required to grant access to public authorities in order to comply with national and state regulations. Also certain existing public information, such as the property location and construction year, will be deemed as non-confidential and

available for viewing without permission.”^[2198] (el resaltado es mío).

Por otro lado, la empresa de *blockchain* Consensus augura un prominente futuro de la cadena de bloques en la gestión de activos inmobiliarios, en el Project financing del real estate, en la securitización hipotecaria, en los registros inmobiliarios, en la planificación urbana, en la identidad digital de inversores e inquilinos, en la automatización de pagos, incluidos los alquileres, y en la gestión contable en real time^[2199].

Específicamente en materia de securitización inmobiliaria, China ya es líder^[2200], con ocho casos exitosos durante 2019. Todos fueron colocaciones privadas, sin oferta pública de títulos valores tokenizados. La *blockchain*, siempre privada, registra las hipotecas y cada pago hipotecario por parte del deudor, dando visibilidad total a los inversores sobre el ciclo de vida del bono emitido. También es muy novedoso e interesante el caso de la empresa Figure^[2201], que en Marzo de 2020 realizó la primera securitización totalmente tokenizada, end-to-end. Los préstamos subyacentes fueron todos originados y registrados en *blockchain*, al igual que los títulos emitidos para securitizarlos^[2202]:

*“Provenance, Figure’s blockchain-based supply chain platform, uses Smart Contracts to enable users to digitally sign and validate critical mortgage documents. The blockchain platform also eliminates the need for parties to repetitively verify data to detect errors or fraud – automating the process and **cutting the cost of back-office functions and intermediaries.** “Blockchain has an almost incalculable potential for unlocking value for the world’s financial markets, and we’re spearheading that transformation by taking on the big challenges like securitization,” said Figure CEO Mike Cagney. “Until now, the industry has been slow to move past white papers and proof-of-concept projects. But **this first-ever production-level blockchain***

ABS achievement importantly underscores that the times are changing.” Other parties involved in the securitization included Jeffries Group (structuring agent, lead underwriter, and warehouse), Nomura Securities International (lead underwriter), Tilden Park Capital (loan contributor and subordinate note buyer), and a large asset manager (senior note buyer). “Nomura is proud to have been a lead underwriter on Figure’s inaugural securitization on Provenance,” said Sanil Patel, managing director of Nomura Securities International. “Provenance is leading the way toward creating a more accessible securitization market, one where smaller issuers may securitize assets at a lower cost than the traditional model.”^[2203] (el resaltado es mío).

6.1.8. Health Care

En el sector salud, la irrupción de *blockchain* también está generando terremotos. Casos de uso aparecen diariamente^[2204]. *Supra* en § 3.4.6.2 se puntualizó como Japón divisa gran potencial en lo relativo a estudios clínicos de nuevas drogas, utilizando la *blockchain* para que los distintos *stakeholders* (empresas farmacéuticas, clínicas de prueba médica, investigadores, universidades y los denominados *contract research organizations*, CROs) puedan compartir información vinculada.

MedRec^[2205], por ejemplo, es un desarrollo del prestigioso MIT Media Lab que inició en 2016 en un hospital de Israel, que combina *blockchain* y *Smart Contracts* para gestionar el acceso a historias clínicas digitales:

“Electronic Health Records (EHRs) were never designed to manage the complexities of multi-institutional, lifetime medical records. As patients move between providers, their **data becomes scattered across different organizations, losing easy access to past records**. As providers — not patients — are the

primary stewards of EHRs, **patients face significant hurdles in viewing their reports**, correcting erroneous data, and distributing the information. MedRec is the combination of a social need with a technological enabler: a system that prioritizes patient agency, **giving a transparent and accessible view of medical history**. To continue the banking analogy, financial systems may contain multiple different depositories of currency, perhaps one for each provider network. The problem is that health records are not fungible; each is an individual's unique imprint. There is no like-for-like trade possible as we can do with money. Whereas competition and multiplicity often results in lower consumer costs, here it risks a mass of incompatible or inaccessible barriers to interchange and control. We propose an alternative: **a distributed access and validation system using the blockchain to replace centralized intermediaries**. The first implementation of Medrec was developed using the Ethereum blockchain. Ethereum uses a system called 'Smart Contracts' to execute scripts on the blockchain, extending bitcoin to a turing-complete language. This system of Smart Contracts significantly broadens the possibilities for decentralised computation using the blockchain, and it is this system which formed the backbone for the development of Medrec.

Smart Contracts act as an intelligent representation that links patients and providers to the addresses of existing medical records. Medrec does not 'store' the record directly; rather encodes metadata that allows records to be accessed securely by patients, unifying access to data across disparate providers. The metadata contains information about ownership, permission and the integrity of the data being requested. The full details of the Smart Contract structure and operation can be found in the technical documentation.”^[2206]
(el resaltado es mío).

Otro desarrollo de *blockchain* y salud es MedicalChain [\[2207\]](#). Este firma desarrolló una *blockchain* fondeada con un token propio ofrecido vía ICO, *MedToken*. Esta plataforma permite y aspira:

“Medicalchain plans to put **everyone in control of their health records and be a partner in their healthcare management**. The pilot (cuatro hospitales ingleses) is the first application for Medicalchain’s platform, **powered by Hyperledger’s open source blockchain technology**, that allows patients to take full control of their healthcare records through blockchain technology and **will provide access to flexible telemedicine services**. Groves’ registered patients will be able to create a **free wallet which will hold and manage access to their health records**. **GP video consultations will also be available to patients, offering the flexibility to see their doctor at a time and place suited to their needs**. The platform will then give patients the **option to pay for services using cryptocurrency**, with users being incentivised to pay for telemedicine services with Medicalchain’s MedTokens.”

En la misma línea se inscribe la *blockchain* de phrOS [\[2208\]](#) desarrollada por el Hospital Universitario de Taipei. Se presentan como:

“the World’s first hospital-wide blockchain integration project; accelerating the collaboration in the healthcare industry by tapping into the benefits of health data sharing while ensuring data privacy. The open architecture empower automated & secure applications to make smart health a reality.”

La empresa FarmaTrust [\[2209\]](#), por su parte, ofrece servicios de gestión de cadena de suministros para la industria farmacéutica, apuntando a eliminar las drogas falsificadas. Se presentan así:

“FarmaTrust has created a **supply chain track & trace solution to meet any serialization requirements from any country and to meet any standards for supply chain events** including GS1 EPCIS event model or extension of it. Now we have an **enterprise solution** to create a full **network effect in the pharmaceutical industry fostering collaboration among various major players in the supply chain but at the same time protecting their competitive interests**. The work for our cost-efficient B2B Zoi exchange is in progress. We have demonstrated our white label capability via OEM relationship by integrating with Systech One. We have provided solution design to Systech One and a confidential client in CT / GT field and used it for Mongolia feasibility study (which is signed off now) by selecting appropriate architecture building blocks from our enterprise platform.” (el resaltado es mío).

Otros casos involucran el seguimiento en *blockchain* de pruebas y ensayos clínicos, como ya lo han propuesto los japoneses. Empresas como Ambrosus [\[2210\]](#) comienzan a diseñar servicios on-chain para esa necesidad, apuntando a los *Deep Pharma Pockets*. El laboratorio Boehringer Ingelheim se asoció con IBM en 2019 para, precisamente, introducir el *blockchain* para la gestión de clinical trials [\[2211\]](#). *Chronicled*, por su parte, es una empresa que ofrece una solución en *blockchain* para gestión de suministros y de inventarios de drogas farmacéuticas, mediante una plataforma llamada MediLedger, que permite:

“**blockchain networks for chain-of-custody in drug supplies**. Thanks to its solutions, **pharmacies can trace back the origins of supplies, detect suspicious, ill-intent activities, like drug trafficking and others, and forged drugs during the process** (...) created MediLedger, a blockchain-based project that allows checking pharma supply chains for conformance with local regulations. In a nutshell, the solution keeps a **forgery-**

proof record of transactions on a blockchain, thus helping to authenticate raw materials that drugs are made of and detect counterfeits promptly. [\[2212\]](#)” (el resaltado es mío).

Se espera que en 2025, el negocio de *blockchain* aplicado a ciencias de la salud formará un mercado de servicios de más de 5.6 billones de Dólares [\[2213\]](#).

6.1.9. *Supply Chain Management (SCM)*

Evidentemente, si la *blockchain* se está utilizando para SCM en la industria farmacéutica, puede ser utilizada en cualquier otra industria a los mismos fines. Ya se ha visto como la industria automotriz y la industria aeronáutica comienzan a testear pilotos on-chain. Los japoneses, por su parte, en § 3.4.6.2 ya han puntualizado un uso muy interesante en materia de logística, para optimizar la trazabilidad de baterías de autos eléctricos, llevando un registro distribuido del *valor residual* de las baterías, las que pueden ser reutilizadas por otras industrias, como la de generación solar, dependiendo de si tienen o no un valor residual mínimo.

Así, Amazon Web Services ofrece servicios “enlatados” de *blockchains* –*Amazon Managed Blockchain*– que sirven para dar trazabilidad a la cadena de producción de cualquier producto. Por ejemplo, Nestlé ofrece en Australia trazabilidad total del café que vende a través de *Chain Of Origin*, utilizando la *blockchain* de Amazon. Con la sola lectura de un código QR en cada paquete, el consumidor puede ver toda la cadena de producción [\[2214\]](#).

Cargill, en Abril de 2020 comenzó a utilizar *blockchain* para dar trazabilidad a sus compras internacionales de *commodities* [\[2215\]](#). Esta fue la primera vez que una compra de *commodities* fue gestionada vía *blockchain*, de punta a punta:

“Tapping into Hyperledger Fabric – an open-source blockchain technology – **US-based Cargill was able to complete the sale**

of a consignment of wheat worth \$12 million to Singapore's Agrocorp in a matter of hours, compared to the several weeks normally required for such a process. **Blockchain tech could prove particularly useful for keeping supply chains open in conditions like those brought on by the Covid-19 pandemic**, given its ability to effectively remove many of the physical touchpoints typically associated with the foodstuffs trade. The shipment between North America and Indonesia was settled on April 1. Participating in the transaction alongside Agrocorp and Cargill were **Dutch financial services provider Rabobank**, Singaporean ship owner Amarante, and shipping agent Transmarine. **Usually, trading a large amount of grain from one country to another is a complex, time-consuming process**. Even when two parties have agreed to do a deal, there's still plenty of work that needs to be done – quality control, shipping, and customs clearance, to name just a few of the steps. The transaction also needs to be financed by banks that can put up the cash. That means that any one trade is likely to involve a lot of players, and a lot of moving parts. **Distributed ledger technologies like blockchain have the potential to streamline this process because they are considered to be secure by design**, increasing trust and traceability with regards to data they store –including information from trade documentation such as letters of credit, waybills, bills of lading, and other contracts.” [\[2216\]](#) (el resaltado es mío).

Walmart, por su parte, lanzó una iniciativa llamada *Food Traceability Initiative*, en la cual utiliza *blockchain* para dar trazabilidad a ciertos productos frescos importados, que son revendidos en sus supermercados [\[2217\]](#). Esto se inscribe dentro de una iniciativa de IBM, la *IBM Food Trust*, que propone el uso de *blockchain* para trazabilidad alimentaria [\[2218\]](#), a través de HyperLedger Fabric, que ya es utilizada por 80 compañías alimentarias y está siendo utilizada para *trackear* 1300

alimentos [\[2219\]](#).

Finalmente, es interesante el caso de la empresa inglesa *EverLedger* [\[2220\]](#), nacida en 2015 de un programa de aceleración del banco Barclays, y que aplica *blockchain* para la trazabilidad de múltiples bienes, como por ejemplo, diamantes [\[2221\]](#). Su solución es:

“The existence of a ledger recording the ownership and origin of the jewels will make them far harder to sell on without recutting to obscure their identifying features or serial code — and lowering their value in the process. Everledger’s ledger is built on the blockchain — the same decentralised record book that underpins bitcoin. It means there’s no one centralised server running things — instead, data is distributed across the network ... Everledger uses the blockchain as its basis because of its immutability...**This permanence is vital in tackling fraud, meaning the ledger cannot be amended later to disguise criminal activity.** Paper certificates for diamonds certifying provenance do already exist, but there’s nothing like Everledger’s ledger, which is continually updateable and accessible from anywhere in the world. 830,000 diamonds have been added to the ledger.” (el resaltado es mío).

6.1.10. Industria del Seguro

El impacto de la *blockchain* en la industria del seguro tendrá similar alcance y profundidad que el impacto que está teniendo en la industria financiera. Así, los veinte líderes europeos de la industria del seguro y del reaseguro formaron un *joint venture* en 2016, constituido en Alemania [\[2222\]](#), y dado en llamar *Blockchain Insurance Industry Initiative* (B3i):

“Formed in 2016, B3i is a collaboration of insurers and

reinsurers aiming to explore the potential for leveraging blockchain technology to provide more fluidity in risk transfer and remove friction and inefficiency in handling transactions (...) to act as a catalyst for the adoption of blockchain standards and to support the transition to a DLT native, digital re/insurance industry.” [\[2223\]](#)

El primer producto de B3i apuntó al mercado del reaseguro inmobiliario. En Febrero de 2020 se realizó la primera operación de reaseguro 100% on-chain [\[2224\]](#), vinculando a 9 aseguradoras con 8 reaseguradoras.

Del otro lado del Atlántico, algo similar está ocurriendo, auspiciado por ACORD, una organización sin fines de lucro que desde hace 50 años autorregula al sector de los seguros, oficiando como una central de datos de la industria, y una creadora de estándares para la industria [\[2225\]](#).

La industria del seguro es menos dinámica –en términos de tecnología– que la industria financiera, aunque evidentemente una retroalimenta a la otra. En 2018, en una conferencia de ACORD se afirmaba que:

“ACORD looked at 1000 insurance change efforts and found that **two-thirds failed**. Pieroni attributed this to the nature of insurers. The companies are built for stability and consistency. **They use the past as a predictor with their legacy claims databases. By nature, people who work at insurers dislike risk and are conservative.** The organizations are full of negative feedback loops. If someone tries something new a typical response is: “We don’t do that here.” What about the third that managed to implement change successfully? A lot address these cultural issues. When looking at issues and opportunities, there must be a focus on positive aspects. “So if you think about blockchain. It can’t just be that it’s some existential threat. There’s a real opportunity here to learn and grow and have impact for our clients,” said Pieroni. There’s the

expected goals and objectives. However, just as important is measuring behavior based changes, addressing those cultural issues. There's the need for the CEO and CFO to commit, but also **you need respected evangelists**. Pieroni commented: "Sometimes there's people that maybe don't have the stripes on their shoulder or the title but really have the informal authority, the credibility to get the organization behind something. These guiding coalitions and who's driving change in the organizations are incredibly powerful." The above culture issue is a big challenge. Another people aspect is the ability to build capacity and competency. Insurers have a hard time attracting top quality talent. Also, **there's tremendous competition for blockchain talent right now**. In the list of criteria for success for technologies, one was integration with existing systems. Changing business processes is a big ask. Based on this experience with the EY Maersk project, Pieroni laid down the gauntlet: "To really get value out of this you have to change your business processes."^[2226] (el resaltado es propio)

Dejando de lado las particularidades culturales del mercado de seguros, B3i fue designada para liderar la comisión de *blockchain* de ACORD:

"The Blockchain Insurance Industry Initiative (B3i) has announced that it will **jointly chair a new Acord project group designed to propose common standards for the adoption of blockchain technology in the re/insurance industry**. Led by B3i and RiskBlock Alliance, the initiative will support the **adoption of data and protocol standards to help re/insurers benefit from the capabilities afforded by Distributed Ledger Technology (DLT)**, applications and networks. "Blockchain has been a great trigger for a new wave of collaboration in the industry and aligns to Acord's core mission," said Bill Pieroni, President and Chief Executive Officer (CEO) of Acord. "We are very pleased that globally all major blockchain initiatives are

built around Acord standards,” Pieroni continued. “We are excited that B3i together with other market participants will be working with us to develop clear, actionable standards around this revolutionary technology.” Susan Joseph, North America Representative for B3i, also commented: “By co-chairing this group, B3i is committed to working with the industry to create standards that will allow for easy adoption. We are delighted that Acord is picking up the mantle and moving forward to promote innovation in Insurance.” [\[2227\]](#) (el resaltado es mío).

En esta línea, Marsh comenzó en 2018 a probar una *blockchain* para la industria, digitalizando los certificados de cobertura [\[2228\]](#):

“Traditionally a Certificate of Insurance is manual and paper-based. **Creating a blockchain digital version can accelerate some business functions such as hiring contractors.** The advantage Marsh has as a broker is the ability to provide proof of insurance for numerous insurer carriers. The broker is collaborating with ISN which works with contractors and suppliers in capital-intensive industries like construction and oil extraction. A part of ISN’s role is to make sure contractors have appropriate insurance. The company helps to manage more than 67,000 contractors in 85 countries. “The insurance industry has been dependent on paper certificates of insurance, manually populated by an insurance agent,” said Brett Parker, technical insurance lead, ISN. **“By digitizing the policy information, we can streamline the process saving our customers time to focus on their core competencies.”**

Marsh is working with IBM and using Hyperledger Fabric. They also have input from ACORD, the insurance data standards body. **The project is currently in pilot phase** and expected to go live later in the year with ISN as the first client. “Vastly simplifying the process for providing proof of insurance is a key enabler of business. IBM is committed to

connecting emerging blockchain networks to facilitate the next generation economy. This is an ideal example of how blockchain can be used on a much broader scale to drive real business results,” said Sandip Patel, general manager insurance, IBM. Sastry Durvasula, chief digital officer at Marsh, commented: “We believe strategic engagements such as this one with IBM, ACORD, and ISN will help accelerate the adoption of further blockchain applications benefiting our clients across industries.”^[2229] (el resaltado es mío)

Muchas empresas comienzan a apuntar al mercado del seguro con soluciones on-chain. Etherisc^[2230], por ejemplo, creó en Suiza –en el cantón de Zug– la Fundación para el Seguro Decentralizado, con el fin de emitir un token para fondar el desarrollo de su plataforma, que permite negociar on-chain riesgos asegurables y celebrar contratos de seguros. Ya ofrecen cobertura de riesgos para el agro, y también para robo de llaves privadas de criptoactivos^[2231]. Se presentan así:

“The Decentralized Insurance Foundation (DI Foundation) is a non-profit foundation organized under the laws of Switzerland, Canton of Zug. Its mandate is to ensure open access to the protocol and platform, provide long-term governance, community, and ecosystem, and be a custodian of funds raised. The DI Foundation is conducting the Token Generating Event. Under US law the DI Foundation is the issuer of the DIP tokens. DIP Tokens act as the **native internal currency that is inseparable from the protocol and network of its users**. DIP tokens are needed to earn transaction fees (% of insurance premiums or fixed cost), incentivize and reward platform users to bring risk to the network, build and maintain risk transfer products. The total supply of Etherisc Tokens is 1 Billion. **DIP tokens give users access to the Decentralized Insurance Platform**. By staking DIP token, participants provide collateral

(bond) to guarantee future performance, availability, and service levels. Staking also signals quality and reputation. As a result, participants can earn money monetizing their skills, software (for example risk models or UI/UX), risk capital, insurance licenses, claim processing, or regulatory compliance/reporting services. DIP stands for the Decentralized Insurance Protocol and also for Decentralized Insurance Platform. **The Protocol provides a permission-less, generic mechanism by which risk of any kind can be priced, serviced, and transferred by a group of independent service providers without having to rely on centralized parties.**”^[2232] (el resaltado es mío)

La empresa Guardtime, a su turno, ofrece seguros on-chain para el transporte marítimo^[2233] en sociedad con Maersk:

“Guardtime recently teamed up with logistics giant Maersk to implement a **blockchain-based maritime insurance platform that will manage risk, use Smart Contracts and establish an immutable chain-of-shipping to help insurance companies thoroughly provide coverage.** The company’s Insurwave platform is poised to manage the insurance processes for more than 1,000 vessels in the first year. The company also expects the platform to oversee more than 500,000 ledger transactions that deal with pertinent maritime insurance information.”^[2234] (el resaltado es mío)

Desde Singapur, la empresa FidentiaX^[2235] creó un marketplace para riesgos asegurables, similar al modelo de Etherisc. Su modelo de negocios propone:

“With FidentiaX, users are able to **buy, sell or store their**

insurance policies on the company's blockchain. Using tokenization, the blockchain-powered marketplace takes existing policies and puts them into the encrypted database. In real-time, users are able to cash out on their policies, buy policies from others or just find all their insurance information in one place. FideniaX recently created ISLEY, a blockchain-powered digital ledger for insurance policies. ISLEY gives customers a complete overview of their insurance policies, notifies them when their premiums are due and displays **an immutable record of your entire policy history.**^[2236] (el resaltado es mío)

Otro caso interesante es el de la aseguradora inglesa AXA^[2237], que en 2017^[2238] lanzó una cobertura por retraso de vuelos 100% en *blockchain*, que ofrece pagos automatizados mediante *Smart Contracts* si los vuelos asegurados sufren retrasos mayores a dos horas:

“When you buy **flight delay insurance** on the fizzy platform, we record the purchase in a tamperproof network, the Ethereum blockchain, making the insurance contract equally tamperproof. **This Smart Contract is connected to global air traffic databases, so as soon as a delay of more than two hours is observed, compensation is triggered automatically.** In this way, AXA has delegated the compensation decision to an independent network, strengthening the trust that customers can have in AXA.”^[2239] (el resaltado es mío)

¿Y qué ocurre en Argentina? Recientemente, en Agosto de 2019, la Superintendencia de Seguros de la Nación (SSN) formalizó, mediante la Resolución N° 733/2019^[2240] la creación de la Mesa de Innovación en Seguros e Insuretech^[2241]. El objetivo es generar una interacción entre los diferentes actores vinculados a la tecnología aplicada al seguro y con ello

promover la innovación de la industria aseguradora. Así, la Mesa de Innovación (o Innovation Hub) es un espacio de colaboración público-privado que busca crear un ambiente de discusión y análisis respecto de tecnologías aplicadas al seguro. Pretende establecer un canal de comunicación que permita conocer nuevos modelos de negocios y tecnologías relacionados con la industria aseguradora, identificar desafíos regulatorios relacionados con riesgos y oportunidades de *Insurtechs*, contribuir a la competitividad del sector y promover los beneficios de la eficiencia y competencia que aportan a la industria.

El primer paso de la SSN fue dado en 2018, con el dictado de la Resolución 219/2018 [\[2242\]](#). Allí, la SSN habilitó por primera vez en la historia del seguro en argentina, *la comercialización y contratación de los seguros de forma digital*.

La Resol. 219/18 dispone, entre otras cosas, que la póliza y demás documentación asociada al contrato de seguro puede ser entregada por medios electrónicos:

“c. Constancia de la entrega de documentación por medios electrónicos:

La documentación deberá remitirse a través de un medio electrónico que permita su lectura, el cual debe incluir el enlace para su descarga.

La entrega por medios electrónicos puede efectuarse a través de:

I. Envío de la documentación por correo electrónico del asegurado y/o tomador, que debe ser declarado al momento de solicitar la contratación, sea esta en forma personal o por medios electrónicos.

II. Puesta a disposición en la página web de la aseguradora, cuya dirección debe constar en los formularios de propuesta del seguro o en la página web por la cual, el asegurado y/o tomador haya solicitado la contratación de la póliza.

III. **Puesta a disposición a través de aplicaciones móviles**, que deben ser indicadas por la aseguradora al momento de la contratación de la póliza.

La entrega de su póliza y/o endosos a través de medios electrónicos no impide la solicitud de la documentación física, si el asegurador o tomador lo requiere.

25.3.2. Las aseguradoras que utilicen los medios electrónicos conforme lo dispuesto en el inciso c. del punto 25.3.1 deberán contar con una página web institucional, mediante la cual en su página de inicio y de manera fácilmente visible se brinde la información acerca de la forma de requerir copia de la póliza u otra documentación contractual, efectuar una denuncia de siniestro, acceder al Servicio de Atención al Asegurado y solicitar la rescisión del seguro.

25.3.3. **Las aseguradoras deben garantizar la inalterabilidad de los contenidos de la información emitida, remitida, transferida o publicada por los procesos de medios electrónicos, particularmente en lo referido a las fechas y numeración correlativa de emisión.** Asimismo, deben adoptar los recaudos necesarios para garantizar la seguridad y confidencialidad de la información procesada por medios electrónicos con sus asegurados.

25.3.4. Las aseguradoras deben conservar y poner a disposición de esta SSN, las constancias que respalden la entrega de la documentación al asegurado, cualquiera sea el medio utilizado.” El resaltado es mío, y hasta altura de la lectura, el lector probablemente coincidirá en que existe una clarísima invitación a disruptar el mercado de seguros con *blockchain*.” (el resaltado es mío)

6.1.11. Registros marcarios

La *blockchain* también presenta casos de uso en la gestión marcaria. La empresa Cognate [\[2243\]](#), ofrece servicios en la *blockchain* de Ethereum, para alojar información marcaria, generando un hash que sirve de prueba de existencia:

“Ethereum is the blockchain network Cognate chose to store trademark data. We developed a series of Smart Contracts that are published to Ethereum and were used in the recording and retrieval of trademark data. With the Ethereum address of your trademark can you can pull up the raw bytecode data that is stored within. Using our Smart Contract code it is possible to retrieve and view said data. This is what our tool does for you.”

6.1.12. *Gestión de derechos digitales*

En materia de gestión digital de derechos, además del caso particular de UJO Music analizado *supra* en § 2.3, es muy interesante el caso de *MediaChain*, una startup de Nueva York del ecosistema *blockchain* que fue comprada por Spotify en 2017^[2244]. El interés de Spotify en la plataforma de *MediaChain* luce claro:

“the startup had developed several technologies (...) including a decentralized, peer-to-peer database to connect applications with media and the information about it, as well as an attribution engine for creators, and a cryptocurrency that rewards creators for their work. In short, the startup was working to leverage blockchain technology in order to help solve problems with attribution.

This is an area where Spotify can use some help, as it turns out. Last year, **Spotify settled a licensing dispute with the National Music Publishers Association (NMPA) in the U.S. over unpaid royalties.** According to the NMPA, **Spotify had failed to obtain mechanical licenses – which refer to a copyright holder’s control over the ability to reproduce a musical work – for a large number of songs on its service, The New York Times had reported.** The issue could impact other streaming services as well, the NMPA said, estimating that as much of **25 percent of the activity on streaming platforms is today**

unlicensed. Spotify at the time agreed to pay over \$20 million to music publishers as a result of this settlement, in addition to a \$5 million penalty. While the company likely avoided several class action lawsuits as a result of the settlement, it spoke to a larger problem in the industry. **Spotify had claimed that it didn't pay out the royalties because it simply didn't have the necessary data to help it figure out whose claims were legitimate, or even how to locate the parties.** It said it lacked an authoritative database that covered all existing music rights. This opens it up to litigation, which is obviously not the ideal way of managing these payments. With [Mediachain](#), Spotify potentially has a solution on its hands – but instead of building out a centralized database with music rights information, it looks like it will build a decentralized one. As [Mediachain](#) explains in a blog post, **its vision for the problem with attribution is a shared data layer, which is says “is key to solving attribution, empowering creators and rights owners, and enabling a more efficient and sustainable model for creativity online.”** It also helps that the team at [Mediachain](#) has music industry experience. The company noted in the post that its CTO Arkadiy Kukarkin was the first engineering hire at the music curation aggregator Hype Machine, and before starting [Mediachain Labs](#), co-founder Jesse Walden had co-founded and run an artist management firm that worked with artists including Solange Knowles, Blood Orange and Majical Cloudz. [Mediachain](#) says it will turn over the technology it had already built to the open source community as it moves to Spotify.” (el resaltado es mío)

6.1.13. *Publicidad digital*

En materia de publicidad digital, la irrupción de la *blockchain* puede ser realmente significativa. El negocio de la publicidad digital es un mercado muy grande, que tendrá un alcanzará un tamaño de casi 500 mil millones de Dólares en 2022 ^[2245]. Se ha sostenido que Google Ads y Facebook Ads,

monopolistas del mercado, han “dibujado” los datos para cobrar más a los anunciantes [\[2246\]](#). Facebook fue “*capturada in fraganti*”, demandada y obligada a pagar 40 millones de Dólares [\[2247\]](#), generando la apertura de sendas investigaciones en Alemania [\[2248\]](#), y también en EE.UU por parte de la *Federal Trade Commission* y el *Antitrust Department* del Department of Justice por supuesta monopolización [\[2249\]](#), además de lograr aglutinar a 47 Procuradores Generales estatales, que están también investigando al gigante tecnológico por sus abusos de posición dominante [\[2250\]](#).

Blockchain puede ser la solución para estas fallas de mercado. Se han identificado [\[2251\]](#) diez ámbitos donde la *blockchain* puede aportar valor: (i) venta directa de avisos digitales sin intermediario mediante plataformas en *blockchain*, desplazando a los monopolistas de siempre, que abusan de su poder de mercado; (ii) detección de fraude: siendo evidente y flagrante como Facebook “dibujó” los números, *blockchain* permite a los anunciantes trazabilidad total en los clicks e impresiones que generan sus avisos, lo que a su vez permite un cobro justo al anunciante, sin que se “dibujen los clicks”; (iii) segmentación eficiente de audiencia digital: “driving an ad campaign according to their customer journey is important. With the help of blockchain, **ad tech platforms can automate campaigns based on the specified set of rules.** If the audience falls into those certain criteria, then only an ad will be visible to them. By doing this advertisers can utilize the budget on better sites to show ads. Audience engagement will be credible now with very **much accurate data that will help design better campaigns.** The leads and subscriptions would be genuine and identifiable; (iv) gestión de datos: la *blockchain* optimiza el proceso de generación de KPIs utilizados para medir el éxito (o el fracaso) de una campaña de marketing digital; (v) customización de los avisos digitales, a medida de cada anunciante: esto permite evitar la “fatiga publicitaria”, al permitir que el anunciante controle, de manera directa a través de una plataforma la frecuencia e intensidad de los avisos –algo hoy imposible debido a los intermediarios centralizados–; (vi) automatización de avisos publicitarios: mediante *Smart Contracts* en *blockchain*, el proceso de subasta de espacios digitales puede ser más

transparente, efectivo y relevante; y (vii) la publicidad *basada en datos* generados en *blockchain* es mucho más eficiente cuando el anunciante tiene acceso directo a esos datos, en lugar de que esos datos queden centralizados en un intermediario, que puede manipularlos en su beneficio. Esto, a su turno, optimiza el cobro y el pago de la publicidad digital y facilita la personalización de contenidos [\[2252\]](#).

6.1.14. *Certificados académicos*

La emisión de certificados académicos también será disruptada por *blockchain*, como lo demuestra una iniciativa auspiciada y acelerada por el MIT desde 2015 [\[2253\]](#), que desde ese año emite certificados digitales en *blockchain* [\[2254\]](#). Desde el MIT afirman:

“Certificates are signals of achievement or membership and some are more important than others. University degrees (a particular type of certificate) can help you get the job you want, or prevent you from getting it if you don’t have the right certificate. **Our current, mostly analog system for managing certificates is slow, complicated, and unreliable.** There are many advantages for creating a digital infrastructure for certificates, but the stakes are high since such a system could grow to represent our professional reputations. We need to be thoughtful about its design, and the type of institutions we trust to govern it (...).

There are many advantages for recipients to have more control over the certificates they earn. Being in control doesn’t mean it would be easy to lie. Similar to the carpenter’s book of references, it should not be possible to just rip out a few pages without anyone noticing. But **being in control means having a way to save credentials, to carry them around with us, and to share them with an employer if we chose to do so (without having to pay, or ask for the issuer’s permission or cooperation).** In order to make that happen we need

an open platform for digital certificates and reputation. Using the blockchain and strong cryptography, **it is now possible to create a certification infrastructure that puts us in control of the full record of our achievements and accomplishments.** It will allow us to share a digital degree with an employer while giving the employer complete trust that the degree was in fact issued to the person presenting it. The blockchain is best known for its connection to the [cryptocurrency bitcoin](#). But in essence it is just a distributed ledger to record transactions. What makes it special is that it is **durable, time-stamped, transparent, and decentralized.**”^[2255] (el resaltado es mío)

6.1.15. Arte y Blockchain

Pero no todo es sólo negocio en el ecosistema *blockchain*. Hay también usos interesantes de la *blockchain* en el mundo de las creaciones artísticas (además del caso UJO Music ya analizado). Por ejemplo, desde la Universidad de Oxford y el Instituto Alan Turing^[2256] y luego de un año de investigación profunda del mercado del Arte, afirman que:

“The application of digital ledger technologies would allow for **verified transaction records and ownership, transparent and fair prices, easier royalty collection, and confirm art pieces’ provenance and authenticity.** Easing the ability to sell quickly and increasing the liquidity is key to unlocking the art market and a distributed ledger-powered art trading platform could provide it. The application of a **transparent, accountable and fair art trading system such as a digital ledger would benefit all parties – artists, buyers and sellers.**” (el resaltado es mío)

En esta misma línea, Christie’s realizó la primera subasta de arte en *blockchain* a fines de 2018^[2257], utilizando la plataforma de *blockchain*

Artory^[2258]. Se dijo en aquélla oportunidad:

“The Artory Registry is the world’s most secure art-centric database, containing highly trusted, vetted data about artworks. Leveraging modern cryptography and blockchain technology to record significant events in the lifecycle of artworks and collectibles, the Artory Registry creates **a secure digital record of transactions, with a goal of providing greater confidence in an artwork’s ongoing provenance and greater efficiency in its eventual resale.** Collectors with artworks registered with Artory maintain anonymity, as their identity is never stored in the Registry.” (el resaltado es mío)

Otro caso interesante es *Auctioneers*^[2259], una plataforma de venta de arte que permite pagar en criptoactivos^[2260]. También existen casos muy interesantes de tokenización de piezas de arte, que permiten el *fractional ownership* comprando tokens emitidos contra el “subyacente artístico”. Así, la plataforma de *blockchain* de arte *Mecenas*^[2261] tokenizó el 49% de una obra de Andy Warhol en 2018, lanzando al mercado Art tokens por un valor de 6.5 millones de Dólares^[2262]. Puesto en otros términos, el dueño de la obra –i.e, del 51% de la obra– monetiza la obra al dividir el dominio, de manera fraccional tokenizada, con un grup de inversores dispuestos a adquirir una “fracción” de la obra, con la expectativa de monetizar su inversión cuando la obra se venda, decisión que quedará siempre a discreción del titular del 51%. De este modo, un activo poco líquido y de inversión restringida para muy pocos, se vuelve líquido –al menos, 49% líquido– y permite invertir en un Warhol comprando un token, en lugar de comprar el (inaccesible) Warhol.

6.1.16. Gestión del talento humano

Ya casi finalizando este “salpicado completamente aleatorio” de casos que

han interesado al autor (y, espero, también al lector), se anotarán algunos casos de uso de la *blockchain* en la gestión del talento humano.

La consultora GARTNER indica en un informe de Agosto de 2019 [\[2263\]](#) que la *blockchain* puede aportar valor a la gestión del talento humano, al menos en cuatro formas distintas: (i) para control de antecedentes laborales: mediante la tokenización de identidades –sumada a la tokenización de certificaciones, ya vista más arriba– se podría eliminar el fraude y la mentira en las postulaciones laborales; (ii) seguridad de datos laborales: el historial de *performance* de un empleado puede ser tokenizado, previa encriptación, y permitir que el empleado comparta información sensible a su respecto con otros posibles empleadores, a la vez que servir de un archivo seguro para el empleador interesado; (iii) automatización de beneficios con *Smart Contracts*: especialmente útil para contratistas y sub-contratistas, los pagos debidos pueden ser automatizados en contratos inteligentes, que sólo liberan los pagos cuando el contratista entrega el material debido, o realiza la tarea debida; y (iv) gestión automática del pago de salarios mediante *Smart Contracts*: a medida que las criptomonedas se vuelvan más populares, más empleados las aceptarán como medio de pago, sea donde sea que residan, incluso en otros países, los *Smart Contracts* permitirán garantizar los pagos cumplidas las condiciones pactadas.

En este sentido, casos de uso muy interesantes en el ámbito laboral son los proyectos implementados por Telefónica de España y BBVA. A fines de 2018, ambas empresas anunciaron que comenzarían a utilizar *blockchain* en el ámbito de los recursos humanos. Así, se utiliza la *blockchain* y los tokens para fomentar la capacitación del personal, premiándolo con tokens a medida que se capacita:

“El proyecto “BBVA Campus wallet” incorpora el uso de los tokens a la actividad del campus virtual corporativo del banco. El proyecto encaja en un modelo de gestión de personas cuyo objetivo es “Que cada una desempeñe el rol adecuado, aporte el máximo valor, alcance el máximo compromiso, aprenda y crezca profesionalmente” y, como herramientas para conseguirlo, establece la formación y el impulso de una cultura

de aprendizaje continuo. El campus virtual incorpora una oferta formativa ajustada a los puestos y mapa de talento organizacional. En este entorno la organización quería generar actividad, reconocer el tiempo que el empleado dedica a formarse o a formar otros... Y la formación adquiere una dimensión que se mide, y hasta otorga capacidad adquisitiva, a través del “**Campus token**”. **El empleado cuenta con un número determinado de tokens que puede ir aumentando a medida que participe en el campus, ya sea realizando cursos o enseñando a otros, y puede “gastarlos” en acceder a otras actividades formativas con un coste determinado.** La formación se convierte, así, en algo muy dinámico, sujeto a las leyes de **un nuevo mercado que recompensa la actualización de conocimientos por parte de los empleados**. Dado que para las compañías la necesidad de actualización de conocimientos es esencial, haber encontrado la forma de facilitarla e incentivarla es realmente un éxito: el éxito de blockchain en formación corporativa. El proyecto Karma de Telefónica, que presentó David Jiménez, está orientado a reconocer el valor de los empleados de la compañía. **Se trata de conceder un agradecimiento real a quienes, con sus actividades extra, aportan valor a la compañía.** Y de nuevo blockchain es la tecnología adecuada para encauzarlo y el concepto de token la respuesta a esta necesidad de reconocer el valor de aquello que realmente es importante, si no indispensable, para la empresa. Esta iniciativa se integrará en la intranet de Telefónica, de manera que **cada usuario contará con un número de karmas que lo posicionará en un nivel determinado.** A medida que vaya realizando aquellas actividades que generan más karmas, irá subiendo a escalones superiores y también **podrá invertir sus karmas en acceder a determinados servicios o actividades.** El proyecto aporta una visión global de la interacción del empleado con las distintas áreas (Formación, Patrocinios, Comunicación, Fundación Telefónica y Personas, entre otras) y permite definir, a la vez, una estrategia global y transparente de reconocimiento. Supone también la posibilidad

de validar el concepto y la tecnología blockchain, de la que Telefónica es pionera, en un escenario cercano y controlable pero de ámbito global. A lo largo del encuentro se mostró cómo la tecnología de la cadena de bloques aporta la solución a muchas de las barreras con las que hoy se encuentran los servicios de formación corporativos. Y es que el funcionamiento tradicional de un servicio de formación, basado en la detección de necesidades, planificación, impartición y medida, no responde ya a las nuevas necesidades de las compañías que, en muchas ocasiones, ni siquiera pueden establecer las competencias técnicas que necesitarán en el futuro más próximo, ni a los actuales hábitos de aprendizaje de los empleados. **En el nuevo escenario la tecnología blockchain aporta trazabilidad, confiabilidad y una unidad de compensación y dinamización que permite hacer explícita cualquier acción que conlleve la generación de conocimiento dentro de la empresa.** Es la herramienta idónea para todos aquellos que defienden que el cometido del servicio de formación debe ser facilitar que el conocimiento interno sea explícito, compartido y crezca a partir del intercambio de experiencias dentro de la organización. Por no hablar de las posibilidades de colaboración que abre entre entidades diferentes, al basarse en un lenguaje y unidades de medida estándares.”^[2264] (el resaltado es mío)

6.1.17. *Blockchain y crisis humanitarias ¿Blockchain en los ojos?*

Finalmente, deben también darse a conocer los valiosos usos de la *blockchain* en contextos de graves crisis humanitarias. En efecto, en 2019 se ha afirmado que más de 50 millones de personas en todo el mundo ha debido migrar en contra de su voluntad por distintas crisis en sus países de origen^[2265], superando a la cifra de migrantes durante la Segunda Guerra

Mundial. ¿Qué puede ofrecer la *blockchain* a tantos millones de personas que han perdido todo, menos la vida? Mucho.

En primer lugar, una identidad digital nueva, ya que en muchos casos han perdido la forma de probarla. Según Noruega, el 70% de los refugiados provenientes de Siria no tienen una forma de identificarse [\[2266\]](#). Existe allí una oportunidad de crear un soporte digital, portable, en un teléfono móvil, que permita acreditar la identidad de los refugiados.

En este sentido, desde el Alto Comisionado de Naciones Unidas [\[2267\]](#) para los refugiados se afirma:

“The increased instability of states and economies underlying the new waves of migration worldwide poses a historic threat to human dignity in many different ways. One very intricate facet of this phenomenon is the weakening — and at times even the loss — of personal identity arising from the fading bonds of citizenship that are frequently the result of the circumstances of migration. Among human groups on the move, **refugees** are particularly affected by this issue. They often find it **enormously challenging to prove fundamental aspects of their identity**. The damage and loss of documentation validating their national identity, their personal data and information, their professional diplomas and so on create **insurmountable barriers to conducting a dignified existence, accessing services and rebuilding their lives**. For many, proof of their identity may still be stored in physical or digital archives within the institutions of their failing state. Alternatively, this **proof may have forever vanished because those institutions have ceased to exist**. The paradox of not owning the proof of your own existence is striking, and it is laden with consequences for refugees. (...) Blockchain technology and strong encryption seem to be new tools for setting up a globally applicable system of digital proofs of identity, relevant for any kind of personal data (birth, health,

citizenship, education and so on). (...) Blockchains take the form of digital public ledgers that are free and accessible for all connected nodes; rather than belonging to a single institution, these ledgers belong to all the users connected to them. Users' identities within a ledger are encrypted and therefore known only to the users themselves. These encrypted and verified identities are not stored on a centralized corporate, governmental or institutional server (ripe for hacking). Instead, **blockchain technology allows personal information to be stored on the relevant decentralized ledger, while cryptographic hashing creates an unbreakable layer of safety.** Digital identities can then be used to conduct 'transactions' among all the users connected to the system. A digital ledger of trusted transactions is maintained for all the participants. The technology is complicated, but the premise is simple: the blockchain establishes trust between independent parties and allows those parties to share trusted information without any intermediary institutions becoming involved. The system works by addressing inherent trust deficits that have developed in our society. Blockchain is not just a distributed ledger but also a distributed consensus ledger through which trust is created by a collectively agreed-upon consensus protocol. **We might therefore be able to prove the birth and provenance of x and y individuals — as well as their qualifications, employment history and so on — even when the institutions that originally provided that proof in the form of certificates no longer exist,** all because of the indisputable verification mechanism that blockchains offer. **Blockchain technology, then, has the potential to create new solutions for refugee and identification systems, providing a digital verification mechanism for people unable to prove their identity, and allowing them to share their identity and transact with other actors.”** (el resaltado es mío)

En materia de *blockchain* e identidad, Finlandia ha decidido implementar la *blockchain* para facilitar el *proceso identitario* de los refugiados que

recibe [\[2268\]](#). Así, desde 2017 cuando un refugiado llega a Finlandia, se les entrega una tarjeta de débito prepaga no bancaria, y la identidad del titular de la tarjeta queda registrada en *blockchain*, lo que permite también llevar un registro de los gastos y consumos de manera anonimizada, y una identidad reforzada *on-chain*, en la *blockchain* de Ethereum. Del otro lado del Atlántico, una startup de Nueva York también propone solucionar el problema de identidad usando *blockchain* para las personas en situación de calle, que ascienden a 60.000 personas en la Ciudad que no nunca duerme [\[2269\]](#). Además de recibir una identidad digital, las personas en situación de calle reciben un teléfono móvil gratuito con una *Wallet* pre-instalada donde se acreditan *tokens* llamados *Change Coins* y también Dólares, los tokens pueden ser cambiados por datos y minutos para hablar. Llamativamente, en EE.UU en 2019 el 11% de la población en edad electoral no tienen una identificación federal válida pero tienen un teléfono móvil.

A febrero de 2020, en el ecosistema de la Organización de las Naciones Unidas hay cinco iniciativas apalancadas en *blockchain* [\[2270\]](#):

“the United Nations International Telecommunications Union and Food and Agriculture Organization have partnered to **track pig supply chains in Papua New Guinea**; the United Nations Capital Development Fund is exploring **blockchain for remittances in Nepal**; and the United Nations Development Programme is using **blockchain to track the cocoa supply chain in Ecuador**. The **Unicef Crypto Fund**, a prototype that lets the agency accept **bitcoin and ether donations** and invest them directly into blockchain startups, was launched in October of last year and immediately had uptake from the cryptocurrency community as a donation of 1 Bitcoin and 10,000 Ether came from from the Switzerland-based Ethereum Foundation (...) one use case that has come to the fore is the use of **blockchain-verified iris scans for Syrian Refugees**. Syrian refugees in Jordan’s Azraq camp are now receiving aid, and paying for their food through a **retina scan that is**

recorded on the blockchain, rather than through ID cards which come with their own issues.” (el resaltado es mío)

El caso de los refugiados Sirios es muy interesante. Repare el lector cómo la *blockchain* puede combinarse con otra tecnología –un lector de iris– para garantizar, de manera indubitada, el destino final de las ayudas humanitarias:

*“The United Nations World Food Programme (WFP) has introduced a pilot project called ‘[Blockchain against Hunger](#)’, deploying **blockchain technology in Jordan’s Azraq camp to make cash-based transfers to 10,000 refugees. WFP relies on biometric registration data provided by the UNHCR and refugees can shop from local supermarkets using [iris scans](#); the system confirms the identity of the refugee in this way, checks their account balance and confirms the purchase. (...)***

“Through blockchain, we aim to cut payment costs, better protect beneficiary data, control financial risks, and respond more rapidly in the wake of emergencies. Using blockchain can be a qualitative leap – not only for WFP, but for the entire humanitarian community”^[2271]

*When refugees shop at a “WFP-contracted supermarket,” Moghraby said, “instead of having a card on them or any ID paper, they’ll just get their groceries, go to a cashier” and **look into an iris scanner. “It communicates with a database that has all the details of the beneficiary, and it confirms that this person is a WFP beneficiary, and then that person can take their groceries and***

go home. The whole process takes about 3 seconds.”^[2272] (el resaltado es mío)

Imagen 15 lector de iris en Siria



<https://www.digitaltrends.com/cool-tech/world-food-programme-building-blocks-iris-scanning-blockchain/>

6.2. *Smart Citizens*

En el apartado anterior se comentaron casos de uso de la *blockchain* en el mundo de los negocios –excepto quizás el caso de la ONU, que es más técnicamente una alianza público privada para el desarrollo–. Pero, a no dudarlo, el verdadero potencial de la *blockchain* y de los contratos inteligentes está en su *uso adecuado por parte del sector público*, y en beneficio de la ciudadanía.

6.2.1. *Voto y Blockchain*

Existen ya desarrollos que aplican la tecnología *blockchain* para la emisión y registro del voto. Es evidente que la *blockchain* puede aportar confianza y

valor a un proceso que genera todo lo opuesto, como es el proceso eleccionario en las democracias del Siglo XXI [\[2273\]](#). Empresas como Blocko [\[2274\]](#) en Corea del Sur ya están testeando pilotos [\[2275\]](#), y comienza a haber mucha literatura especializada en el tema [\[2276\]](#). La revolución del voto electrónico en *blockchain* ya está en curso [\[2277\]](#), aunque también se han puntualizado los riesgos de ciertas aplicaciones que están ya en el mercado y no son tan seguras [\[2278\]](#). Empresas como *Voatz*, *Votem* y *Smartmatic-Cibernetica* [\[2279\]](#) ya han realizado votaciones on-chain [\[2280\]](#).

6.2.2. Participación ciudadana on-chain: el caso Alcobendas

Un interesante piloto de participación ciudadana on-chain se desarrolló por una firma catalana, Marketpay.io [\[2281\]](#), implementado en el Ayuntamiento de Alcobendas del Reino de España, y presentado como ponencia al IV Congreso de Ciudades Inteligentes [\[2282\]](#). Este piloto es muy interesante por varios motivos. El primero, porque involucra al sector público, el Ayuntamiento de Alcobendas, que ha tomado la decisión de “apalancarse” en la tecnología y la Innovación para potenciar la transparencia e incentivar la participación ciudadana. En segundo lugar, el caso bajo estudio permite descentralizar las votaciones de los ciudadanos en procesos de presupuestos participativos, recurriendo a un registro distribuido inmutable, auditable, seguro y confiable, e introduce el concepto de *Smart Citizen*. De modo tal que, una alianza público-privada “apalancada” en la tecnología *Blockchain* permite pensar (y crear) Ciudades y Comunidades Sostenibles y a la vez darnos Paz e Instituciones Sólidas.

A continuación, se describen muy superficialmente los puntos salientes:

- 1) El proceso participativo está basado en varios tipos de

preguntas: selección simple, múltiple o de valoración con el fin de distribuir votos entre distintas opciones. Las preguntas pueden tener fichas descriptivas y el proceso participativo debe tener un inicio, un fin y seguir las guías de estilo institucionales.

2) La aplicación podrá ser utilizada en cualquier dispositivo web.

3) Hay un censo de votantes dinámicos que son los ciudadanos de Alcobendas, respecto de los cuales rigen ciertos requisitos de seguridad: autenticación fuerte a través de los mecanismos que ofrece el Ayuntamiento, votos únicos e inmutables, proceso fácilmente auditable y anonimato.

4) Desarrollo de una aplicación de Votación y Oráculo de Identidad: esta aplicación es la encargada de que el proceso de votación esté completamente descentralizado. Contiene el front-end que permite al usuario votante visualizar la votación concreta a llevar a cabo, e incorpora el wallet de identidad en Ethereum desde donde emite su voto. Desde la DApp se da acceso al nodo de la red Ethereum en el que reside el *Smart Contract*. Por su parte, el Oráculo de Identidad se encarga de autorizar a los wallets como votantes en el *Smart Contract*. Por tanto, la DApp se presenta al oráculo para que éste le conecte con los Servicios del Ayuntamiento de Autenticación y Autorización y active o deniegue el derecho al voto. Dichos servicios municipales incluyen la identificación con certificados, tarjeta de Alcobendas, Cl@ve y Consulta al padrón municipal para comprobar si un usuario es vecino de Alcobendas y a qué distrito pertenece. Mientras la identidad digital de usuario votante no resida en un sistema descentralizado donde él mismo sea soberano de dicha identidad (i.e., SSID, algo que ya está dando que hablar...), se deberá operar mediante un oráculo de identidad como el descrito anteriormente. Debe resaltarse que cada voto es encriptado por medio de claves que solo pueden descifrar los “recontadores”, logrando así que el proceso de votación sea secreto. Estos recontadores son usuarios conocidos cuyas

cuentas de Ethereum son publicadas oficialmente. El Ayuntamiento conoce al votante, pero no lo puede cruzar con los votos, y el recontador conoce el voto, pero no lo puede cruzar con los votantes.

5) Faucet de Fondos para la votación. La DApp debe disponer de fondos (una pequeña fracción de Ethers) para poder pagar la minería de la red pública de Ethereum que conlleva la emisión del voto. Para ello se ha programado un servicio independiente (API) que puede ser invocado por la DApp para aprovisionarse de dichos fondos justo antes de llevar cabo el gasto, o sea, cualquier acción que implica minado. La aplicación evita así al usuario la compra de Ethers, cosa innecesaria cuando se trata de un proceso de participación ciudadana.

6) Aplicación de Recuento: Esta aplicación es la encargada de que el proceso de recuento de votos esté completamente descentralizado. Esta DApp sigue la misma arquitectura que la anterior. En este caso el front-end permite identificar a aquellos usuarios que hayan sido definidos con el de “recontador” de votos e invocar el *Smart Contract* para descargar las votaciones y descifrar las papeletas (si está así configurado) y realizar el recuento. Terminado el plazo de la votación, unos usuarios determinados por la organización para ser “recontadores” podrán cerrar la votación y solicitar el recuento (i.e., la llamada al Contrato Inteligente para ir contabilizando los votos que se han realizado). La votación puede ser configurada para ser completamente anónima al Ayuntamiento. Esto conlleva que la DApp de Votación cifre asimétricamente cada voto con las claves públicas del o los recontadores.

7) Contrato Inteligente en Ethereum encargado de la lógica y registro de los votos y votantes. El *Smart Contract* es capaz de registrar cada una de las tipologías de preguntas de los requerimientos, pero es agnóstico a las preguntas concretas de una votación específica. El contrato ofrece funcionalidades de cara al votante, al Ayuntamiento y a los recontadores. Cada

funcionalidad es un end-point que va identificado en Ethereum con un hash único.

8) Una vez que el usuario ha accedido a la aplicación desde su móvil o navegador, se inician los siguientes pasos: (i) Autenticación del usuario y Autorización a votar: las autorizaciones serán encargadas al pool de oráculos trabajando en round-robin que acceden al *Smart Contract* para validar los wallets de identidad como votantes; (ii) Contestación a las preguntas por parte del usuario: el usuario contesta cada una de las preguntas y cada contestación será guardada localmente en una estructura de datos (JSON) conformada para la votación; y (iii) Votación: el usuario consentirá la votación pulsando el botón para ello. Esto conlleva la ejecución del Contrato Inteligente enviándole las contestaciones a las preguntas (voto). La estructura de la votación puede estar cifrada o no según esté determinada en la configuración de la votación. El votante dispone de un comprobante del voto, del identificador de la transacción y el enlace para la visualización directa en el *Blockchain*.

9) Finalmente, en cuanto a los costos de aplicación de esta tecnología, se deben pagar los costos de minería de cada transacción (i.e., de cada emisión de voto). El costo de la minería depende de: (1) *gas price* ^[2283] ofrecido a la red de minería y (2) tamaño del bloque a minar. El costo de un voto cifrado rondaba, a 2018, los 2,81€. Sin embargo, dada la fluctuación del Ether y su costo en Euros, se deberían analizar soluciones del tipo *Blockchain* permissionado, de desarrollo propio, y con o nulo coste de transacciones.

El caso analizado permite pensar esquemas de *blockchain* B2G que pueden aportar una importante (y necesaria) cuota de legitimidad, transparencia y solidez a las instituciones públicas, y generar un mayor involucramiento del Ciudadano en la gestión de la cosa pública, dando nacimiento a una era de *Smart Citizens*.

6.2.3. Compras públicas on-chain

Otro ámbito importante de aplicación de la *blockchain* es en materia de compras públicas. En un muy interesante trabajo publicado en 2018, Freya Hardwick, Konstantinos Markantonakis y Raja Akram [\[2284\]](#) afirman que la *blockchain* puede permitir diseñar un ecosistema de compras públicas seguro y transparente, en el cual realizar todo el proceso de licitaciones públicas, dándole la posibilidad de controlar el proceso a los ciudadanos. Los autores incluso proponen una arquitectura en tal sentido para un *blockchain* que corra en Ethereum [\[2285\]](#).

La OECD, a su turno, en un informe también de 2018, titulado *Blockchains Unchained: Blockchain Technology and its use in the Public Sector* [\[2286\]](#), afirma que:

“Blockchain transactions can be used as a means of documenting every transfer of an asset from its origin. Governments could track an asset from its creation, through potentially multiple stages of transportation, and eventually through purchase and even managing asset inventory. This gives anyone with permission the ability to view the chain of custody (e.g., government officials, the public) and thus enables trust in the asset (Yaga, 2017). Potential examples include tracking food, medicines, natural resources such as diamonds, and many others from origin to distribution (...) This enables the potential for Blockchain technology to be leveraged as a tool for transparency and accountability in government spending, which is often executed through federal contracts. Things such as tracking and paying vendors, managing purchase commitments and transactions, and monitoring schedule performance could all be done in a way that is accessible to all relevant players, as well as the public, as appropriate. In addition to the transparency and accountability

angle, Blockchains can make government contracting more efficient by eliminating a significant amount of overhead and automating processes that lend themselves to the logical “if/then” workflows of Smart Contracts. [\[2287\]](#),”

El informe de la OECD resalta un caso puntual de Méjico, que está desarrollando a nivel federal una plataforma en Ethereum que combina *Smart Contracts* y digitaliza todo el proceso de compra pública, dejando un registro inmutables [\[2288\]](#). En el Reino Unido, por su parte, desde la UNIVERSIDAD DE CAMBRIDGE se señala que la tecnología tiene potencial para estos fines, pero se afirma que se utilizarán probablemente *blockchains* privadas y no públicas [\[2289\]](#), con protocolos de gobierno del tipo PoS o PoA, y no PoW. Repárese que también existen investigaciones que afirman que la *blockchain* no ofrece una genuina solución al problema de las compras públicas [\[2290\]](#). En EE.UU, la *General Services Administration* comenzó en 2017 a aplicar *blockchain* para el proceso de compra pública bajo ciertos contratos estandarizados, utilizando *Smart Contracts* [\[2291\]](#). En un informe de 2019 de la DATA FOUNDATION [\[2292\]](#) se analizaban ya siete proyectos en *blockchain*, algunos vinculados al public procurement –otros con otro enfoque– por agencias tan disímiles como la FDA, la Administración de Niños y Familias, el Departamento del Tesoro, el Departamento de Salud y Servicios Humanos, así como la nombrada GSA.

Nuevamente merece resaltarse a la institucionalidad de Chile, que ha sido el primer país de Latinoamérica en probar un piloto de *blockchain* para el sector de compras públicas, utilizando la cadena de bloques como un notario para cada paso del proceso de compras. El innovador proceso es liderado por la agencia de compras públicas más respetada de toda Latinoamérica, como es ChileCompra, verdadero ejemplo a seguir [\[2293\]](#), en sociedad con el BID.

A su vez, desde varios bancos de desarrollo regionales se promueve cada vez más la investigación en materia *smart procurement*, toda vez que la corrupción endémica en muchos de los países asistidos por este tipo de

instituciones podría eliminarse o reducirse apalancando el proceso de compras en *blockchain* [\[2294\]](#).

Otro caso interesante es el de Aragón, en el España, cuyas Cortes han tratado en 2018 un proyecto de ley, dado en llamar Proyecto de Ley de Organización y Uso Estratégico de la Contratación Pública [\[2295\]](#), donde se habilita expresamente la utilización de sistemas electrónicos de *registro distribuido* –i.e. DLTs– para incrementar la transparencia y asegurar la integridad de la información en materia de contratación pública. Reza el proyecto bajo análisis:

“Disposición adicional cuarta.— Utilización de registros distribuidos.

1. Para asegurar la integridad de los datos y documentos que consten en cualquier expediente, procedimiento o registro de contratación pública de cualquier clase, podrán implementarse sistemas electrónicos de registro distribuido.

2. También podrán utilizarse, con plena validez legal, sistemas electrónicos de registro distribuido para la automatización de trámites o procesos que se realicen en el seno de procedimientos de contratación pública de cualquier clase.

3. A los efectos de lo dispuesto en esta disposición, tendrá la consideración de sistema electrónico de registro distribuido el que permita el almacenamiento de la información, o su representación digital mediante huella electrónica, de manera permanente, simultánea y sucesiva en una base de datos distribuida, de manera que quede garantizada la inmutabilidad de dicha información y se permita la auditoría de su integridad.” [\[2296\]](#)

Finalmente, en Argentina, a fines de 2019 la Lotería de Río Negro anunció que estudiaba utilizar *blockchain* para *certificar* procesos internos del ente [\[2297\]](#).

6.2.4. Registros inmobiliarios

Un informe de 2019 elaborado por la Comisión Europea [\[2298\]](#) analizaba el caso de Georgia, que en 2016 decidió replicar íntegramente su registro inmobiliario en la *blockchain* de Bitcoin, en el proyecto conocido como *Exonum* desarrollado por la empresa BitFury [\[2299\]](#). Este innovador concepto permite que los ciudadanos puedan tener acceso a un certificado digital de su propiedad, redundante con el título físico, que sigue siendo válido. Se describe el proceso de este modo:

“Blockchain technology is used by citizens to validate property-related certificates and by notaries to make new registrations. At the moment of writing (Q2 2018) the service allows for the **registration of purchases and sales of existing land titles and a registration of new land titles**. In the future, the system will be extended to a registration of property demolitions, mortgages and rentals and notary services (Shin, 2017).

Only the National Agency of Public Registry (NAPR), notaries and Georgian citizens can participate in transacting, so it is a **permissioned blockchain**. The blockchain system is private with regards to who can validate the transactions. The **actual transaction validation occurs by a group of known servers or nodes. The transaction data is then hashed and recorded on the public Bitcoin blockchain**, which creates transparency of the existence of the land title for all citizens. Therefore the system is a **mix between a public permissioned and private permissioned blockchain**. This hash is a cryptographic proof that transaction details match with the data recorded on the private blockchain, without actually seeing it. The consortium governance is centralized, as NAPR can decide on the direction of the consortium and Bitfury is the technology provider. The blockchain-based land title registry implementation is mature,

meaning that the verification of the transaction occurs via the public blockchain network. **Since April 2016, over 100,000 land titles have been registered using the technology.** The Exonum protocol can **handle up to 5000 transactions per second (tps) between the private nodes.** Hence, the adopted blockchain solution does not have bottlenecks related to registration. This blockchain deployment offers a mixture of quantitative and qualitative benefits:

- A significant reduction of the land title registration and verification time. Whereas **in the past these actions took around 1 to 3 days to process, the transaction time using blockchain has been reduced to a matter of minutes;**
- Increased transparency in the registration process of land titles;
- Increased reliability for citizens driven by the accuracy of the data stored at NAPR;
- Efficiency gains realised in the ecosystem, as the time to verify a certificate has been reduced from a matter of days to a matter of seconds;
- **Operational costs were reduced up to 90% for the land title registering service.**

The costs involved in the implementation of the new system are mainly non-recurring, related to the customization of Exonum protocol and the integration with NAPR and the notaries. These costs, borne by NAPR, include:

- The development cost of a custom-built protocol based on the Exonum framework. There was no hardware cost, as NAPR did not need to buy additional infrastructure;
- The maintenance and operation costs of Exonum blockchain;
- The organisational capacity cost to prepare NAPR to understand and utilize blockchain technology;
- Transaction cost related to anchoring transactions on the Bitcoin blockchain. As transactions are anchored in groups, fees are paid not on per transaction basis but periodic ally. The

actual levels of these cost items were not disclosed. **Citizens are not charged any extra fees.** It is noteworthy, that several cost items that existed in the old system are still present, as the blockchain system does not substitute the legacy solution. These items are related to the maintenance of a central digital record system. Also the check-up of a request initiated by citizens is still manually done by a notary.

The process of adding or changing a land title can be characterised by the following steps: (1) A citizen can initiate a request to the service-hall or a notary for the registration or verification of a land title extract, just as in the traditional system. (2) The notary registers the land title on the private Exonum blockchain. (3) Hashes of the private Exonum blockchain are anchored on the public Bitcoin blockchain. This guarantees the integrity of all transactions in the Exonum blockchain, up to the latest anchored block in the Bitcoin blockchain. (4) **NAPR provides the citizen a digital certificate of their asset, supported with the cryptographical proof of the originality of the extract, published on the Bitcoin blockchain.** (5) The only difference from a citizens' perspective is that they can now check if a land title is legitimate. This can be done by any Georgian citizen.”^[2300] (el resaltado es mío)

En esta misma línea, Suecia ha anunciado su interés en utilizar *blockchain* en materia registral^[2301] y ha realizado las primeras pruebas en 2018^[2302], utilizando *Smart Contracts* que son *GDPR-compliant*.

6.2.5. *Blockchain y cobro de impuestos*

Un informe de Deloitte del año 2017^[2303] señalaba que la *blockchain* presenta potencial también para el cobro de impuestos. Se afirmaba en ese informe:

“Blockchain has the power to disrupt and strongly reorganize accounting and the way tax payments are processed. As the technology is still in its infancy, introducing Blockchain to the tax authorities would require a revolution in both governmental databases and network systems. The effective implementation of Blockchain for taxes is not only limited to this area and requires considering every are of governmental activity. Asides from integrating IT systems on many levels, it is clear that implementing Blockchain would also require far-reaching changes to the legal system, reforming laws on databases, intellectual property and legal identity. However, the benefits of Blockchain technology on a governmental level are hard to overlook. **In the long run, Blockchain can be a driving factor in implementing real-time, automated tax processes for both small and large enterprises.**” [\[2304\]](#) (el resaltado es mío)

Así, se auguran usos “fiscales” para la *blockchain*, en materia de percepción de aportes y contribuciones patronales, *transfer pricing* y recaudación del IVA. Con relación al primer caso de potencial uso, desde Deloitte afirman:

“In the majority of developed countries, **matters related to payroll are mostly digitalized.** However, the systems for payroll taxes have a significant flaw: there are many government institutions involved and each one holds their own register, de facto duplicating data held by other institutions. Implementing a Blockchain - based to a situation where employers will not need to act as intermediaries, responsible for calculating and transferring tax and social security payments from employee salaries to relevant institutions. **This can be done for example by embedding Smart Contracts that fully automate the process,** which could be done in the following steps:

1. The employer inserts the gross amount of salary into the

system,

2. Within the Blockchain system (limited only to the tax administration, banks and the other necessary parties), tax data is matched with the payment

by Smart Contract technology and calculates the correct tax and social security amounts,

3. The net salary is automatically transferred to the employee's account and the calculated tax to the government,

4. As a result, the payroll tax process is faster and less costly and cash-flow is more efficient.”^[2305] (el resaltado es mío)

Con relación al *transfer pricing*, desde Deloitte se afirma:

“According to United Nations data, intra firm trade makes up around 30% of global trade altogether. The laws regulating transfer pricing are different for each country, requiring that cross border transactions between related parties comply with arm's length price. Simply put, this price should mirror the proposed or applied price between non-related parties in an open market. How could Blockchain benefit transfer pricing regimes?

- A Blockchain distributed ledger that makes it easy to track the flow of transactions and identity of all involved parties.

- The agreements are written into a self-executing Smart Contract.

- All movements on the Blockchain are time-stamped and cryptographically sealed, eliminating the possibility of tampering.

- Each information is stored on the Blockchain and visible to parties that have access to the Blockchain.

- The payments are executed by a smart-contract if they meet the specified conditions.”^[2306] (el resaltado es mío)

Finalmente, en relación al IVA, desde Deloitte afirmaban en 2017:

“Currently VAT is the key driving factor of tax administrations and **the largest contribution to governmental budgets**. For these reasons tax authorities search for ways of more effective VAT collection in order to gain more revenue and shorten the budget gap. The most advanced solutions are present in Brazil, where electronic invoices are mandatory and received by tax authorities in real time. European countries such as Hungary are also planning to implement real-time reporting solutions (Hungary from 1 July 2018). Next in line is Poland, where the Ministry of Finance is working on everyday reporting of JPK_VAT (electronic reporting based on the OECD’s SAF-T). On a European Union level, VAT is also the center of attention with the proposed large reform of the EU VAT system in the upcoming years. In the current state of VAT - on both national and international level, the system is fraught with a variety of problems. It is **highly reliant on businesses themselves to correctly calculate the amount of VAT due** and submit it to the tax authorities, which is a **burden especially to SMEs**. There are two main reasons for this: tax returns and settlements are calculated over a fixed period, for example monthly or quarterly, and the calculations are not based on actual transactions, but rather on arbitrary dates (for example invoice dates). In addition, the system makes it difficult for governments (if not impossible) to track VAT payments, resulting in MTIC, MTEC and carousel fraud. In an international context, controlling VAT data is troublesome as each country maintains their own ledgers, making it difficult to obtain wholesome data on VAT movements. How can Blockchain benefit everyday VAT transactions? a) The administrative burden of companies is significantly reduced, saving time and the cost of accounting services, b) All of the transactions are conducted in real-time, c) All the transactions executed by Smart Contracts are tamper proof and transparent, d) Reduced risk of fraud and mistakes, e) Immediate insight into a company’s finances, f) High speed of

money transfers between businesses and the government, g) Taxpayers get the burden of VAT amount calculations on invoice level and VAT amount due on tax return level taken away, h) Room for VAT frauds is drastically reduced because the same system allowing for processing VAT from transactional point of view, allows at the very same time for multi-dimension checks and verifications of the transaction, parties of the transactions and legal and business context of the transaction.”[\[2307\]](#) (el resaltado es mío)

6.2.6. *Homeless ID: el caso de Texas*

Finalmente, con un caso de uso similar al comentado *supra* en § 6.1.17, debe traerse a colación un piloto desarrollado en *blockchain* desarrollado en Texas [\[2308\]](#), que apunta a mejorar la identidad de las personas en situación de calle [\[2309\]](#). En una nota publicada en Techcrunch en Abril de 2018 se afirmaba:

“The goal of the city’s blockchain pilot program is to consolidate the identity and vital records of each homeless person in a safe and confidential way while providing a means for service providers to access that information. Adler explained that “there are all kinds of confidentiality issues that arise when you try to do that, so the thought was that blockchain would allow us to bridge that need.”By using blockchain, the hope is that the city could replace paper records, which are hard to manage, with electronic encrypted records that would be more reliable and secure. In addition, the blockchain platform could create a decentralized authentication mechanism to verify a particular person’s identity. For instance, a homeless services worker operating in the field could potentially use their mobile device to verify a

person live, without having to bring someone back to an office for processing. More importantly, vital records on the blockchain could build over time, so different providers would know what services a person had used previously. Majid provided the example of health care, where it is crucially important to know the history of an individual. The idea is that, when a homeless person walks into a clinic, the blockchain would provide the entire patient history of that individual to the provider. “Here was your medical records from your last clinic visits, and we can build off the care that you were given last time,” he said. Austin is partnering with the Dell Medical School at the University of Texas to work out how best to implement the blockchain for medical professionals.”^[2310]

VII. Uniendo Los Puntos

7.1. Convertir la Información en Conocimiento

Hemos llegado al final del viaje. ¿Mucha información, no? Intentemos ahora convertirla en *conocimiento*. Primero, un rápido repaso.

En el **CAPÍTULO I** de este Manual se buscó sintetizar los antecedentes filosóficos de la *blockchain*, ya que es importante siempre conocer las intenciones que subyacen a las acciones (y a las innovaciones). Se dieron algunas definiciones de las DLTs y de la *blockchain*, y se analizaron sus características esenciales –decentralización, mecanismos de consenso, e inmutabilidad salvo *hard forks*– y sus distintos tipos –abiertas, privadas, híbridas–. Se analizaron las discusiones que surgieron con la Internet de la *Información*, y se predicó su reedición ante la irrupción de la nueva Internet del *Valor*. Se comentaron también las limitaciones de la *blockchain*, el uso de las mismas asociado a criptomonedas, el boom y el crack del *cryptomarket*, y el surgimiento de las CBDCs, con China liderando ampliamente.

En el **CAPÍTULO II**, a su turno, se abordaron los contratos inteligentes y se analizaron distintas definiciones desde Nick Szabo en adelante. Se puntualizaron las teorías en torno a su naturaleza jurídica, y se los comparó con los *Computable Contracts* y los *data-oriented contracts*. Se analizaron sus rasgos principales: observabilidad, verificabilidad, privacidad y ejecutabilidad automática. Se analizaron algunos casos de uso, incluyendo los *Smart Contracts híbridos*, y se analizó la cuestión de la identidad digital, la anonimidad y la pseudonimidad en virtud del encriptado asimétrico de llaves públicas y privadas. Se analizó para qué pueden servir los *Smart Contracts*, y para qué no podrán servir, *desmitificándolos* al resaltarse las dificultades existentes y los puntos críticos, tales como la codificación deficiente, las limitaciones del lenguaje computacional *vis-à-vis* el lenguaje técnico legal, y los problemas vinculados a su revisión judicial. Se plantearon los principales modelos de Justicia Distribuida, y se resaltaron algunos usos actuales de los Contratos Ricardianos. También se presentó a las redes de *Smart Contracts*, desarrollándose el concepto de las *Dapps*, *DOs*, *DAOs* y *DACs*, y se analizó el caso *TheDAO*, se presentó *TheLAO*, se adelantaron nociones sobre la

estandarización en materia de *Smart Contracts* y se auguró el inicio de la *Década de las DAOs*.

En el **CAPÍTULO III**, se combinaron los conceptos dados en los primeros dos Capítulos, y se comenzó con el análisis –que se extiende hasta el Capítulo V– de las interrelaciones entre la *blockchain*, los tokens, los *Smart Contracts* y el Derecho.

Así, en primer término se analizaron tres escenarios posibles, con sendos ejemplos: la evasión hostil (*SilkRoad*), la alineación eficiente (*RegTech*) y el alivio de fricciones transaccionales (STOs, ICOs, DAICOs y IEOs). Seguidamente, se presentó la *Taxonomía del Token* y se profundizó en los STOs y ICOs, pasando por los SAFTs y el proceso de venta de tokens y también de su reparto gratuito vía *airdrops*. Se profundizó también en la tokenización, se analizaron sus beneficios, así como sus riesgos y sus desafíos y se la comparó con la securitización.

En segundo término, se introdujo un estudio del Derecho Comparado en relación a los criptoactivos y los *Smart Contracts*. En este sentido, se analizaron los muy importantes avances en el Reino Unido, cuyo sistema jurídico está liderando ampliamente la recepción de los criptoactivos y *Smart Contracts*. Se analizó también el caso de EE.UU. tanto a nivel federal como estatal, incluyendo el análisis de legislación proyectada a nivel federal, y algunas leyes estatales muy interesantes, como el caso de Vermont, Wyoming y Delaware. También se hizo foco en las regulaciones existentes en Singapur, Suiza, España, Japón, Francia, Corea del Sur, Francia, Méjico y Chile. Se resaltó el abordaje regulatorio suizo, francés y mejicano, y también se puntualizó como Japón está abordando la responsabilidad de *Exchanges* y *Wallets* a nivel legislativo.

En tercer término, también en el **CAPÍTULO III** se analizó la interrelación de los criptoactivos y los *Smart Contracts* con el Derecho Nacional vigente. Así, se analizaron primero las diversas teorías en punto a la naturaleza jurídica de los criptoactivos, conceptualizándolos como un bien mueble incorporal registrable. Se analizó también su encuadre, dadas ciertas circunstancias, como títulos valores no cartulares atípicos, dada la libertad de creación que existe en dicha materia. Se analizó también la regulación del crowdfunding, y el desarrollo y las características de la *Blockchain* Federal

Argentina. Luego, se encuadró a los *Smart Contracts* como contratos electrónicos, puntualizándose su eventual encuadre como contrato adhesivo. Se valoraron distintas opciones de reflejo contable de los criptoactivos y se contrastó el Estatuto del Consumidor con los *Smart Contracts*, desarrollándose los ámbitos donde pueden surgir conflictos. Se señalaron también las posibles tensiones que pueden surgir entre la *blockchain*, los *Smart Contracts* y el régimen de Defensa de la Competencia, el Régimen Falencial y el Régimen de Protección de Datos Personales. Finalmente, se incluyó también una muy breve disgresión sobre las decisiones basadas en datos, el *Machine Learning*, y conceptos como *Explainability* y *Unsupervised Machine Learning*, a la vez que se puntualizó la ausencia de un tratamiento legislativo sobre la *blockchain*, los criptoactivos y los *Smart Contracts* a la fecha en que este Manual se escribe.

En el **CAPÍTULO IV** el foco se puso en las cuestiones contractuales y en delinear los trazos gruesos de la responsabilidad civil emergente en entornos *blockchain*.

Así, en primer término se presentó la teoría de la conexidad contractual *off-chain*, analizándose sus clases, modalidades y sus efectos, y se postuló su posible aplicación a los entornos *on-chain*.

En segundo término, se analizaron ciertas particularidades de los contratos celebrados para programar un *Smart Contract*, de los servicios de auditoría de software, y se indagó en la naturaleza jurídica contractual que se anuda entre los usuarios de criptoactivos, *Smart Contracts*, y los *Exchanges* y *Wallets*. Se analizaron casos de ciberataques sufridos por *Exchanges* y *Wallets*, y se hizo foco en los contratos de licencia de software y en las cláusulas de limitación de responsabilidad que suelen contener. Se analizó también la reciente regulación argentina de las billeteras digitales de dinero electrónico, fenómeno *relativamente próximo* a las *Wallets* de criptoactivos.

En tercer término, también en el **CAPÍTULO IV** se introdujeron nociones del *Legal Design*, y se auguró para ésta disciplina un gran desarrollo de la mano de los *Smart Contracts* en particular y los contratos electrónicos en general. Se finalizó el **CAPÍTULO IV** analizando cómo el Derecho Privado a nivel comparado comienza a acomodarse para receptor esta nueva *Internet del Valor*. Se analizaron posturas de Derecho Comparado en relación a la

responsabilidad objetiva, la cláusulas de liberación de responsabilidad, y los seguros obligatorios, analizándose algunos casos importantes que han llegado a los Tribunales. Se presentó la teoría de la responsabilidad por riesgo creado, se analizaron sus fundamentos como factor de atribución, y se brindaron y visualizaron unas primeras reflexiones preliminares en torno a la responsabilidad civil en entornos de *blockchain*.

En el **CAPÍTULO V** se analizaron los primeros pasos regulatorios en Argentina hacia el entorno *blockchain*, de la mano del BCRA y CNV. También se recordaron nociones elementales de los mercados de dinero *fiduciario* regulados en Argentina, tanto a nivel bancario como de mercado de capitales, y se analizaron las principales *innovaciones jurídicas* de las últimas dos décadas en dichos ámbitos, desde la negociación bursátil de cheques de pago diferido, pasando por la regulación de los contratos derivados, hasta la desmaterialización de títulos valores con oferta pública y las facturas de crédito electrónicas. Seguidamente se pasó revista a los avances y criterios regulatorios comparados, puntualizándose muy especialmente en las posiciones de la SEC, IOSCO, FinCEN, FINRA, y CFTC, y analizándose el caso puntual de la legislación Maltesa.

El **CAPÍTULO V** concluyó presentando los nuevos desafíos que genera la tributación digital. Se ofreció una muy breve revisión de la tributación de los criptoactivos a nivel comparado, y se analizó en particular la tributación de los criptoactivos en Argentina, resaltándose que el Congreso sólo se ha referido a los mismos *a los fines de gravarlos* en 2017, mediante la Ley N° 27.430, pero desde ese momento no ha habido otro avance legislativo para regularlos, promoverlos, o prohibirlos.

Finalmente, el **CAPÍTULO VI** buscó ilustrar al lector con casos de uso de la *blockchain*, de los criptoactivos y de los *Smart Contracts* tanto a nivel empresarial como gubernamental

7.2. Una obligación moral y ética

Durante cuarenta y cinco días de cuarentena en mi querida Ciudad de Córdoba, he intentado sistematizar toda la información que he ido recabando

desde Noviembre de 2017, cuando la UNIVERSIDAD CATÓLICA DE CÓRDOBA me designara como primer Director Ejecutivo del recientemente creado CENTRO DE EMPRENDEDORISMO E INNOVACIÓN (CEINN-UCC).

El CEINN-UCC está radicado en su Escuela de Negocios de la UNIVERSIDAD CATÓLICA DE CÓRDOBA, el *Instituto de Ciencias de la Administración –ICDA–* que fue creado en 1978 por el aquél entonces Provincial de la Compañía de Jesús en Argentina, el Padre Jorge Mario Bergoglio, por consolidación de los preexistentes *Centro para el Perfeccionamiento en Administración de Empresas* –el CEPADE, creado en 1967, el primer centro de formación en *Management* del interior del país–; del *Centro de Investigación para la Administración Pública* –CIPEAP, creado en 1972–; y del Centro de Investigación para la Administración Cooperativa –CIPAC, creado en 1977–.

En el ICDA también dirijo desde 2014 el Curso de Posgrado en Derecho Empresarial y la nueva Maestría en Derecho de Empresas. En Diciembre de 2019, el Colegio de Abogados de Córdoba creó una nueva Sala de Derecho y Tecnología, designándome Director. El objetivo de la nueva Sala es acercar el Derecho a las Tecnologías.

En estos tres años a cargo del CEINN-UCC he aprendido mucho, de la mano de grandes *Creadores de la Innovación* que han pasado por el CEINN-UCC, y también de grandes juristas, como el Dr. Thibault Schrepel, con quien tuve el honor de cursar la primera cohorte de la *Blockchain Summer School* dictada en la UNIVERSIDAD DE UTRECHT en Junio de 2019.

Como dije al iniciar este Capítulo, es importante *siempre* conocer las intenciones que subyacen a las acciones.

En mi caso, la intención no es otra que tratar de volver *simple* algo muy *complejo*, y por y para ello decidí escribir este Manual. La simplicidad es la máxima sofisticación, y dejaré que el lector juzgue si he cumplido o no con mi declarada intención, la que considero una obligación *moral y ética* en mi rol docente, desde hace ya 15 años cuando me incorporé como Ayudante en la Cátedra de Filosofía del Derecho del Dr. Armando Andruet (h), en la Facultad de Derecho y Ciencias Sociales de la la UNIVERSIDAD CATÓLICA DE CÓRDOBA.

Como se dijo al inicio de este Manual, el Abogado del Siglo XXI necesita una gran cuota de *Astucia Legal* ^[2311] para navegar aguas turbulentas, aguas de cambios disruptivos, producto de las cuatro innovaciones incrementales – algunas fundacionales, otras experimentales– que están en su infancia o adolescencia, pero que madurarán en la próxima década, y se combinarán entre sí en modos que aún no hemos diseñado. Me refiero a la Inteligencia Artificial, el *Blockchain*, el Internet of Things –incluyendo el Industrial Internet of Things, *IIoT*– y la Computación Cuántica. En este sentido, empiezan ya a pensarse combinaciones entre Inteligencia Artificial y *Blockchain*, que permiten dejar registrado en *blockchain* el proceso de aprendizaje de los algoritmos, de modo tal de poder rápidamente detectar errores en el entrenamiento de algoritmos ^[2312] y corregir sus sesgos.

En palabras de Alegría ^[2313], ya citado, nuestra cultura jurídica no sólo no puede quedar encandilada por grandes luces, sino que está encomendada a *usar el ingenio* para recibir y mejorar lo que se decante de precedentes computables, debiendo desarrollar la *Ars Combinatoria* que requiere de una inventiva propia, de una generación de *nuevos recursos técnicos* que sirvan para nuestras comunidades en el actual estado de su desarrollo. Es falsa (o al menos ingenua) la creencia que sostiene que la *blockchain*, sus plataformas, protocolos y sus funcionalidades pueden operar completamente “*al margen de la Ley* ^[2314]”.

Como también se afirmó antes, a medida que que la tecnología de la cadena de bloques permee en sectores que abracen sus ventajas y funcionalidades, los sistemas legales de todo el mundo (y los Abogados y Jueces que en ellos operan) deberán, en un momento u otro, identificar, evaluar y definir cómo resolver los conflictos que se susciten entre los que operan dentro de la red, y fuera de ella ^[2315]. *Y habrá casos fáciles, casos difíciles y casos importantes.*

El desafío es encontrar un justo equilibrio entre, por un lado, esta tecnología de enorme potencial y, por el otro, el sistema legal y social donde se inserta, resguardando *pari passu* las garantías constitucionales de ejercer industria con fines lícitos, asociarse, innovar y emprender, y, por el otro, la paz social.

Para ello, la relación entre Derecho y *Blockchain* debe ser colaborativa y de diálogo asertivo, lo que requiere que abogados y programadores hablen un mismo idioma.

Como también se afirmó antes, estoy absolutamente convencido que la educación legal actual no está a la altura de las habilidades y competencias que se demandarán al Abogado del Siglo XXI. Es innegable que la formación de grado en Derecho no acentúa la innovación, ni la agilidad ^[2316]. Tampoco es común que se *mezclen* contenidos legales y tecnológicos en los trayectos formativos.

Pues bien, los signos de los tiempos indican que deben vincularse intrínseca y funcionalmente los trayectos formativos del Derecho y las Ciencias de la Computación muy rápidamente, ya que en poco tiempo la industria legal será *uno de los sectores más impactados por las nuevas tecnologías*. La disrupción del sector legal vendrá de la mano del *LegalTech*, combinado innovaciones *inter-tecnológicas* con el Machine Learning, la Legal Automation, el Bid Data aplicado, y la *Blockchain* y los *Smart Contracts*.

Se ha afirmado que esta *combinación* de tecnologías producirá impactos cada vez más frecuentes y más intensos, que afectarán lenta pero persistentemente la forma de ejercer la profesión de Abogado en el Siglo XXI ^[2317], profesión que deberá conocer y manejar nuevos conceptos y nuevas disciplinas tales como la *Lex Cryptographia* acuñada por Wright y De Filippi, o el *Legal Programming* acuñado por Koulu, y utilizar cada vez más la visualización contractual mediante el *Legal Design* que impulsa la Universidad de Stanford desde su LEGAL DESIGN LAB ^[2318] para facilitar el acceso a la Innovación para todos los *Usuarios* de la *Innovación*.

7.3. Aceleración

Ahora bien, si algo quedó en claro por la crisis global desencadenada por el COVID-19, es que la *Economía del Conocimiento* ^[2319] y la *Digitalización del Estado* ^[2320] debieran acelerarse como Políticas de Estado.

Para ello, es necesario también que el Derecho se *digitalice* muy rápidamente, para que pueda útilmente acompañar esta Revolución Industrial 4.0 [\[2321\]](#) que ya *no tendrá freno*, y que, sin dudas, producirá enormes cambios económicos y sociales en todo el mundo, que se *suman* a los que va a producir el COVID-19.

Martin Wolf, columnista económico del prestigioso *Financial Times*, ha sostenido que hasta cierto punto todo esto es nuevo, y que si bien una pandemia *era* posible, nunca podríamos anticipar exactamente *cómo sería o cuándo ocurriría*. Afirma que probablemente el COVID-19 causará una catástrofe de la que quizás no nos recuperaremos por décadas, produciendo una gigantesca crisis política, social y económica, cuyos efectos durarán mucho más allá de la crisis sanitaria [\[2322\]](#).

Ante tal contexto adverso, se postula que la *reconstrucción* de la Economía y de los Gobiernos debiera apalancarse fuertemente en la Tecnología –más específicamente en la *blockchain*– si es que se quiere aumentar su resiliencia. Esto será esencial para prepararnos como Sociedad para enfrentar, de manera más eficiente, nuevas pandemias o eventos similares que son previsibles pero inevitables [\[2323\]](#).

Pero es muy, muy importante que el árbol no *tape* el bosque: no debe perderse de vista que el verdadero y esencial desafío planetario es frenar el *Cambio Climático* [\[2324\]](#), cuyos efectos probables *hoy* son aún inciertos en punto a cuándo se presentarán, pero no debe dudarse que se *producirán*.

En este sentido, esta pandemia debe vivirse como un tremendo entrenamiento para el partido verdadero, del cual la civilización humana puede no sobrevivir si no se prepara. Deben *drásticamente* acelerarse las Finanzas Sustentables y aplicar la Tecnología es la única forma de hacerlo.

Sin dudas, acelerar la *digitalización* (del Derecho, de los Gobiernos y de la Economía) traerá consigo otros grandes riesgos [\[2325\]](#), pero el principal de ellos es quizás que nadie debiera *quedar afuera* de la digitalización por incomprensión, por falta de capacidad, o por no entender *cómo funciona* una

tecnología.

Es muy importante que nadie quede afuera de la Innovación y que todos *puedan ser Usuarios de la Innovación*. Los Abogados debemos estar al lado de los *Creadores de la Innovación*, pero también al lado de los *Usuarios de la Innovación*, especialmente al lado de aquellos más desfavorecidos, a los que les toca vivir un mundo que será cada vez más digital. *Más Digital* puede ser sinónimo de *más Inclusión*, como se ilustró con el caso de los refugiados Sirios, donde la *blockchain* puede combinarse con otra tecnología –un lector de iris– para garantizar, de manera indubitada, el destino final de las ayudas humanitarias.

El Covid-19 impondrá –por la fuerza y el dolor– la necesidad de (re)construir la Economía (y a los Gobiernos), y ello nos pone ante una oportunidad única de apalancarnos fuertemente en la Tecnología, para (re)construir resiliencia y estar mejor preparados para nuevas pandemias o eventos similares que el *Cambio Climático inexorablemente* va a producir, aunque se desconozca con precisión cuándo ocurrirán.

A tal fin, la *blockchain* y los *Smart Contracts* como tecnología subyacente y facilitadora –*enabling technology*–, más temprano que tarde, cambiará para siempre la forma en que intercambiamos *valor*, así como Internet transformó drásticamente la forma que se intercambiaba *información*.

Creo que no debe dudarse: las bondades y los beneficios que la desintermediación, la descentralización, la transparencia, la auditabilidad y la inmutabilidad pueden traer son enormes, tanto en la esfera empresarial como en la esfera gubernamental.

Ahora bien, para que la Economía Digital pueda acelerar su paso, se requieren antes importantes definiciones de Política de Estado que la República Argentina debe rápidamente evaluar y decidir, se demandarán grandes inversiones públicas y privadas en infraestructura, educación y talento humano, serán necesarias muchas modificaciones legislativas y regulatorias que afectarán intereses creados de muchos sectores profesionales y empresariales, deberán debatirse en la Academia nuevas definiciones legales, y, principalmente, deberemos asumir y reconocer que la situación general de nuestra Sociedad puede ser *mejor que la actual*, si apostamos

firmemente por la innovación y la digitalización en y de los Gobiernos, de la Economía, y del Derecho ^[2326].

Los Abogados también podemos (y debemos) *innovar* para acompañar a los *Creadores* de la *Innovación*, con el foco siempre puesto en que nadie se quede afuera y en que todos accedan al efectivo ejercicio del derecho a ser *Usuarios* de la *Innovación*. Al lector que ha llegado hasta aquí se le ha impuesto la misma obligación moral y ética de quien suscribe.

[1] Confr. World Economic Forum, *Deep Shift: technology tipping points and societal impact*, p. 24 recuperado el 05/05/2020 en http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report y Thibault Schrepel, *Libra: a concentrate of "Blockchain Antitrust"*, publicado en Michigan Law Review (online), Abril de 2020, disponible para descarga el 16/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3574684, p. 160.

[2] Confr. Gartner, Inc., *The real business of blockchain*, escrito por David Furlonger y Christophe Uzureau, y publicado en 2019 por Harvard Business Review Press, p. 3, disponible para su compra online aquí: <https://www.gartner.com/en/publications/the-real-business-of-blockchain>.

[3] Confr. Constance E. Bagley, *What's Law got to do with it? a Systems approach to Management*, disponible al 17/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=898652. Afirma Bagley que la *astucia legal* permite y fomenta el diálogo *Legal-to-Management*, una comunicación asertiva y efectiva entre managers y sus asesores legales, un trabajo en conjunto para resolver problemas complejos, integrando las consideraciones legales en la formulación y ejecución de estrategias para proteger y potenciar los recursos de la empresa. La astucia legal es un valioso proceso managerial, una práctica de capacidades dinámicas para acompañar empresas que construyen ventajas competitivas en un "*mundo de competencia Schumpeteriana basada en la innovación, la rivalidad de precios y performance, dividendos crecientes, y la "destrucción creativa" de competencias actuales*".

[4] Confr. Rob May, *Emerging problems in AI, and Blockchain as a solution*, disponible al 05/05/2020 en <https://hackernoon.com/emerging-problems-in-ai-and-blockchain-as-a-solution-19c04883b642>.

[5] Confr. Héctor Alegria, *El Derecho Privado hoy y la innovación jurídica*, LA LEY

29/05/2013, Cita Online: AR/DOC/2014/2013.

[6] Confr. Dennis Kennedy y Gwynne Monahan, *Lawyers get ready, there's a blockchain coming*, recuperado el 11/04/2020 de <https://www.lawpracticetoday.org/article/lawyers-blockchain/>.

[7] Se sigue general del orden expositivo de Dennis Kennedy y Gwynne Monahan, o.c.; de Caitlin Moon, *Blockchain for lawyers 101:Part 2*, recuperado el 11/04/2020 de <https://www.lawtechnologytoday.org/2017/01/blockchain-lawyers-101-part-2/>; de Brent Miller, *Smart contracts and the role of lawyers (part 3) – About lawyering transactions on blockchains*, recuperado el 11/04/2020 de <http://biglawkm.com/2016/10/25/smart-contracts-and-the-role-of-lawyers-part-3-about-lawyering-transactions-on-blockchains/>; y de Jaliz Maldonado, *10 ways blockchain technology will change the legal industry*, recuperado el 11/04/2020 de <https://www.natlawreview.com/article/10-ways-blockchain-technology-will-change-legal-industry>.

[8] Ampliar en <https://www.smartdubai.ae/initiatives/blockchain> recuperado al 11/04/2020.

[9] Ampliar en Miguel Ángel Bustos Argañaraz, *El tracto sucesivo y sus modalidades*, recuperado el 11/04/2020 de <http://escribanos.org.ar/rnotarial/wp-content/uploads/2015/09/RNCba-46-1983-08-Doctrina.pdf>.

[10] Ampliar en <https://legalconsortium.org>, y en <https://entethalliance.org/legal-industrys-role-in-the-future-of-blockchain-2/> recuperados el 11/04/2020.

[11] Ampliar en <https://kleros.io/es/> recuperado al 11/04/2020.

[12] Confr. Federico Ast, *Kleros, un protocolo de justicia para Internet*, recuperado el 11/04/2020 en <https://medium.com/kleros/kleros-un-protocolo-de-justicia-para-internet-920c28a588f1>. Otra visión en la misma línea del *blockchain-based-ADRs* es la propuesta por Andreas Antonopoulos y Pamela Morgan, a la que bautizaron *Decentralized Arbitration and Mediation Network*, confr. <https://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key> recuperado el 11/04/2020.

[13] Nota del autor: si Ud. está leyendo esta nota, es porque al igual que Ast anticipa efectivamente una masificación del uso de contratos inteligentes. Si, además, su profesión es la Abogacía, entonces también descuenta la gran cantidad de conflictos que se generarán cuando esa masificación tenga lugar.

[14] Confr. Federico Ast, *Kleros, un protocolo...o.c.*

[15] Confr. Karen Yeung, en *Regulation by blockchain: the emerging battle for supremacy between the Code of Law and Code as Law*, publicado en *Modern Law Review*, Marzo de 2019, Vol. 82, número 2, p. 239.

[16] Ibid.

[17] Confr. Kevin Werbach, en *Trust, but verify: why the blockchain needs the law*, publicado en *Berkeley Technology Law Journal*, 2018, Vol. 33, número 2, p. 550.

[18] Confr. Mark Fenwick, Wulf A. Kaal y Erik Vermeulen, *Legal education in the blockchain revolution*, recuperado el 21/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2939127.

[19] Idem, p. 5.

[20] Idem, p. 6. Sostienen los autores citados, en opinión que se comparte: “*Increasingly, legal work, such as contract drafting, legal risk management, and dispute resolution, will be outsourced to technology and robots. **Lawyers and legal advisors will increasingly assume the role of project managers and business advisors.***” El resaltado es mío.

[21] Véase *infra* nota 43.

[22] Véase *infra* nota 326.

[23] Véase <https://law.stanford.edu/organizations/pages/legal-design-lab/>

[24] Confr. <https://www.coinspeaker.com/china-dcep-digital-yuan/>, disponible al 10/05/2020.

[25] Confr. Alan Cunningham, en *Decentralisation, Distrust & Fear of the body – the worrying rise of crypto-law*, en *Scripted*, Volumen 13, número 3, diciembre de 2016, p. 240, recuperado el 01/04/2020 de <https://script-ed.org/article/decentralisation-distrust-fear-of-the-body-the-worrying-rise-of-crypto-law/>.

[26] Confr. Stuart Haber y W. Scott Stornetta, *How to Time Stamp a Digital Document*, en *JOURNAL OF CRYPTOGRAPHY*, en Enero de 1991, ya sostenían que existía una necesidad de certificar la fecha en que un documento había sido creado, o modificado. Esta “estampa de tiempo” será luego utilizada en Bitcoin.

[27] Se ampliarán estos conceptos en § 2.2.3.1 más abajo.

[28] Confr. <https://www.activism.net/cypherpunk/manifesto.html> recuperado el 01/04/2020.

[29] Ibid.

[30] Confr. Alan Cunningham, en *Decentralisation...* o.c. p. 242.

[31] Confr. Wei Dai, *B-Money*, recuperado el 01/04/2020 de <http://www.weidai.com/bmoney.txt>.

[32] Confr. David Chaum, *Blind signatures for untraceable payments*, publicado en *Advances in Cryptology*, David Chaum, Ronald Rivest y Alan (editores), 1983, Ed. Springer, New York, p. 199-203, citado por Marc Pilkington, en *Blockchain technology: principles and applications*, recuperado el 15/04/2020 en <https://www.semanticscholar.org/paper/Blockchain-Technology%3A-Principles-and-Applications-Pilkington/e31ca71621e1402a46ac2c1afb2eba9a7061d139>. Para una noción ampliada del problema del doble gasto y cómo blockchain lo resuelve, véase Toshendra Kumar Sharma, *How blockchain is solving the problema of double-spending in the finance sector?* Recuperado el 15/04/2020 en <https://www.blockchain-council.org/blockchain/how-blockchain-is-solving-the-problem-of-double-spending-in-the-finance-sector/>.

[33] Confr. Wei Dai, *B-Money*, recuperado el 01/04/2020 de <http://www.weidai.com/bmoney.txt>

[34] Confr. Marco Iansiti y Karim R. Lakhani, *The truth about blockchain*, Harvard Business Review, enero de 2017, p. 4, señalan su utilización en el marco de ARPAnet, al amparo del Departamento de Defensa de EE.UU.

[35] Nathan Fulmer, *Exploring the legal issues of blockchain applications*, publicado en Akron Law Review, Enero de 2019, Vol. 52, número 1, p. 162.

[36] Confr. Kevin Werbach, *The song remains the same: what cyberlaw might teach the next Internet economy*, publicado en Florida Law Review, Febrero de 2018, Volumen 69, número 3, p. 900.

[37] Ibid. La declaración de Barlow puede leerse aquí: <https://www.eff.org/es/cyberspace-independence>, disponible al 01/04/2020. Se volverá sobre esto en el Capítulo III.

[38] *In re* “A & M Records, Inc. v. Napster, Inc.”, 239 F.3d 1004, 1029 (9th Cir. 2001).

[39] *In re* “United States v. Microsoft, Inc.” 87 F. Supp. 2d 30, 35 (D.D.C. 2000);

[40] Confr. Marco Iansiti y Karim R. Lakhani, *The truth about...* p. 5.

[41] Ibid.

[42] Ampliar en Yochai Benkler, *The Wealth of Networks*, disponible el 01/04/2020 en http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf.

[43] Confr. Aaron Wright y Primavera De Filippi, *Decentralized blockchain technology and the rise of Lex Cryptographia*, p. 4, recuperado el 01/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

[44] Sobre innovaciones incrementales, ampliar en <https://hbr.org/2018/09/reevaluating-incremental-innovation> recuperado el 01/04/2020.

[45] Confr. Aaron Wright y Primavera De Filippi, *Decentralized blockchain technology and the rise of Lex Cryptographia*, p. 4, nota 15.

[46] Véase *infra* en § 1.1.8.2.

[47] Aaron Wright y Primavera De Filippi, *Decentralized...* p. 5.

[48] Ibid.

[49] Ibid.

[50] Confr. Kevin Werbach, en *Trust, but verify: why...* p. 489.

[51] Confr. Amy Cortese, *Blockchain technology ushers in the “Internet of Value”*, disponible al 01/04/2020 en <https://newsroom.cisco.com/feature-content?articleId=1741667>

[52] Confr. Marco Iansiti y Karim R. Lakhani, *The truth about...* p. 5.

[53] Ibid.

[54] Confr. Marc Pilkington, en *Blockchain technology: principles and applications*, recuperado el 15/04/2020 en <https://www.semanticscholar.org/paper/Blockchain-Technology%3A-Principles-and-Applications-Pilkington/e31ca71621e1402a46ac2c1afb2eba9a7061d139>

[55] Ibid.

[56] Idem, p. 7.

[57] Ibid.

[58] Confr. Aaron Hankin, *Bitcoin pizza day: celebrating the \$80 million pizza order*, recuperado el 01/04/2020 en <https://www.investopedia.com/news/bitcoin-pizza-day->

[celebrating-20-million-pizza-order/](#).

[59] Confr. https://en.wikipedia.org/wiki/Nick_Szabo.

[60] Confr. Nick Szabo, *The idea of Smart Contracts*, recuperado el 01/04/2020 en https://web.archive.org/web/20060615044959/http://szabo.best.vwh.net/smart_contract

[61] Confr. Nick Szabo, *BitGold*, recuperado el 01/04/2020 en <http://unenumerated.blogspot.com/2005/12/bit-gold.html>

[62] Confr. Nick Szabo, en <https://cointelegraph.com/top-people-in-crypto-and-blockchain/nick-szabo> recuperado el 01/04/2020.

[63] Confr. Karen Yeung, en *Regulation by blockchain...* p. 214.

[64] Ibid.

[65] Ibid.

[66] Confr. Lawrence Lessig, *Deja vú all over again: thinking through law & code, again*, conferencia brindada en el *Sidney Blockchain Workshop*, Diciembre de 2015. Video disponible al 01/04/2020 en <https://www.youtube.com/watch?v=pcYJTIbhYF0>

[67] Ibid. Lessig avizora que habrá muchos conflictos entre la blockchain y la regulación, algunos más importantes que otros, y otros tantos, evitables. La intensidad de los conflictos dependerá de la arquitectura de cada blockchain.

[68] Confr. George Coulouris, Jean Dollimore, Tim Kindberg y Gordon Blair, *Distributed Systems – Concepts and Designs*, 5ta. Ed., Ed. Addison-Wesley, 2012, Boston, p. 2.

[69] Para analizar las diferencias y cosas en común entre sistemas distribuidos y DLTs, véase Rajesh Nair, *Why aren't distributed systems engineers working on blockchain technology?* Recuperado el 1/04/2020 en <https://eng.paxos.com/why-arent-distributed-systems-engineers-working-on-blockchain-technology>.

[70] Confr., BBVA, *Cuál es la diferencia entre una DLT y "blockchain"?* recuperado el 01/04/2020 en <https://www.bbva.com/es/diferencia-dlt-blockchain/>.

[71] Ibid. Para una descripción de las seis tecnologías que usualmente utilizan todas las blockchains, puede ampliarse en Michael Flaxman, *The blockchain is evolutionary not revolutionary*, recuperado el 01/04/2020 de <https://eng.paxos.com/the-blockchain-is-evolutionary-not-revolutionary>.

[72] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 489, nota 1. Por convención,

se emplea Bitcoin con mayúscula cuando se quiere hacer referencia a la cadena de bloques subyacente, en tanto software y protocolos que viabilizan dicha plataforma puntual y abierta; y se emplea bitcoin con minúscula para hacer referencia a unidades individuales de la criptomoneda que corre en la plataforma Bitcoin.

[73] Confr. Gartner, Inc., *The real business of blockchain*, escrito por David Furlonger y Christophe Uzureau, y publicado en 2019 por Harvard Business Review Press, p.10.

[74] Ibid. Se indican allí las diferencias entre blockchain y una base de datos: éstas sirven para almacenar información con fines generales; la información en ellas contenida es editable, se puede borrar, modificar, etc. y si bien una base de datos puede estar distribuida entre varios partícipes, siempre tiene un único administrador central que la controla. En blockchain, el control sólo se materializa en el consenso.

[75] Confr. Aaron Wright y Primavera De Filippi, *Decentralized...*p. 7, nota 27. Cada nodo de la blockchain de Bitcoin aloja una copia de la cadena de bloques más larga, y sólo se aceptan nuevos bloques cuando la transacción es válida y el bitcoin en cuestión no ha sido previamente gastado. Este atributo vuelve a la blockchain muy resiliente, ya que la misma copia de la cadena está alojada –encriptada– en todas las computadoras de la red, y no en un servidor central, de modo tal que si alguna o algunas computadoras fallan, es posible que la base de datos compartida sea rápidamente recreada en su totalidad.

[76] La función de *hash* toma datos entrantes de cualquier tamaño, y devuelve un hash de un tamaño determinado –generalmente de menor tamaño que los datos entrantes–. Esta función de hashing permite generar un atributo denominado *collision resistance*. El SHA256, que es el acrónimo de *Secure Hash Algorithm 256* fue publicado por primera vez en 2001. Se trata de un algoritmo que contiene un proceso matemático computarizado que genera una secuencia aleatoria de 256 bits (64 caracteres alfanuméricos), cualquiera sea el input que recibe. El hashing vuelve la información ilegible. Alex Preukschat, en *Qué es y de qué sirve el algoritmo SHA-256 en el Protocolo Bitcoin?* recuperado el 01/04/2020 en <https://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm/> sostiene que un algoritmo de encriptación (o cifrado) tradicional es una función que transforma un mensaje en una serie ilegible aparentemente aleatoria, usando una clave de encriptación que puede ser revertida (es decir, obtener el mensaje original) sólo por quienes conocen dicha clave. Por medio de la encriptación, la información privada puede ser enviada públicamente por internet sin mayor riesgo de que otros puedan tener acceso a ella.

[77] En el consenso mediante PoW, ciertas computadoras de la red, llamadas *mineros*, deben resolver problemas matemáticos complejos, mientras que otras computadoras

corroboran que la solución dada no corresponda a una transacción previa. Para justificar la inversión en poderosas computadoras afectadas al PoW, el primer minero que resuelva el problema asociado a un bloque nuevo, obtiene como recompensa nuevos bitcoins que se emiten, y el derecho a cobrar *transactions fees*. Aaron Wright y Primavera De Filippi, *Decentralized...* p. 7, nota 29.

[78] Confr. Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (Agosto 7, 2015), disponible al 18/04/2020 en <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>. Buterin define a las blockchains consorciadas como “*a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered “partially decentralized”.* “**Fully private blockchains: a fully private blockchain is a blockchain where write permissions are kept centralized to one organization.** Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.” El resaltado es mío.

[79] Citado por Marc Pilkington, en *Blockchain technology: principles..o.c.*, quien sostiene que, adrede, Buterin no hace referencia a las palabras como registro, dinero, o transacciones, ya que quiere puntualizar que la esencia de la blockchain es la información y los procesos, y no debe limitarse a la esfera monetaria, y de hecho, la blockchain puede existir sin haber emitido un token o una moneda. Esta posición es rechazada por otros criptoexpertos, que afirman que la moneda nativa es una parte esencial del sistema de incentivos de la red para mantener su seguridad. Pilkington concuerda con Buterin, en el sentido de que la criptoconomía o la finalidad de pago generalmente asociada a la blockchain, no son atributos esenciales de la blockchain, sino características de las blockchains más populares.

[80] Confr. Eliza Mik, *Smart Contracts: terminology, technical limitations and real world complexity*, publicado en *Law, Innovation and Technology*, volumen 9, número 2, p. 275.

[81] Confr. Karen Yeung, en *Regulation by blockchain..* p. 210.

[82] Confr. Yeung, o.c., nota 12, con razón señala que la inmutabilidad es relativa, ya

que es posible bifurcar (*fork*, en inglés) una blockchain, mediante el copiado de su código y la distribución posterior de una versión modificada. En este caso, la versión vieja y la versión nueva del software pueden coexistir si existen nodos que sigan utilizando la versión anterior, pre-bifurcación. Kevin Werbach, en *Trustless Trust*, p. 67, recuperado el 03/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757380 sostiene que una bifurcación crea dos cadenas de bloques incompatibles entre sí, ya que los mineros de una cadena no reconocerán las transacciones agregadas por los mineros de la otra cadena. En su obra, en nota 292, afirma que Bitcoin fue bifurcada en tres oportunidades debido a errores de programación (*bugs*) que permitían el doble gasto u otros ataques.

[83] Confr. Kevin Werbach, en *Trustless Trust*, p. 2, recuperado el 03/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757380

[84] Confr. Max Raskin, en *The law and legality of smart contracts*, publicado en 1 GEO. L. TECH. REV. 305 (2017), p. 317.

[85] Confr. Jared Arcari, en *Decoding Smart Contracts: technology, legitimacy & legislative uniformity*, en Fordham Journal of Corporate & Financial Law, 2019, Vol. 24, número 2, p. 367.

[86] Idem, p. 369.

[87] Confr. Nathan Fulmer, *Exploring the legal...o.c.* p. 166.

[88] Confr. Nick Szabo, *The dawn of trustworthy computing*, recuperado el 07/04/2020 en <https://perma.cc/Z7YL-F5XB>.

[89] Ibid.

[90] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en The Business Lawyer, Primavera 2019, p. 10. Los mismos autores también esbozan otra definición, menos técnica, pero valiosa, en la página 36 de la obra citada: “*The blockchain is a mere collection of agreed upon calculations by decentralized computer systems. The blockchain is merely an idea reached by the consensus of computation; it is pure information, contained only in the mathematical rules of its inception and the sum of the computation. The blockchain is entirely maintained and owned by a distributed group of anonymous users located throughout the planet who would not likely recognize or comply with any legal authority*”.

[91] Confr. BID y Foro Económico Mundial, *Windows of Opportunity: Facilitating trade with blockchain technology*, White Paper, Junio de 2019, recuperado el 04/05/2020 de http://www3.weforum.org/docs/WEF_Windows_of_Oppportunity.pdf, p. 10.

[92] Parlamento Europeo, *How blockchain technology could change our lives*, estudio en profundidad realizado por Philip Boucher, Susana Nascimento y Mihalis Kritikos, Febrero de 2017, disponible al 05/04/2020 en [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA\(2017](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)

[93] Confr. Thibault Schrepel, en *Collusion by Blockchain and Smart Contracts*, publicado en Harvard Journal of Law & Technology, otoño 2019, Vol. 33, número 1, p. 117.

[94] Idem, p. 124, señala que el rasgo de inmutabilidad o irreversibilidad es lo que le da valor genuino a la blockchain, y la diferencia de cualquier servicio de cloud computing on demand, como Amazon AWS.

[95] Véase *infra* en **1.1.9.1.**

[96] Ampliar en Chris Coverdale, *A beginner's guide: private and public key cryptography deciphered*, recuperado el 15/04/2020 en <https://medium.com/coinmonks/private-and-public-key-cryptography-explained-simply-4c374d371736>.

[97] Decir que algo está *hasheado*, significa que es el resultado (*output*) de una transformación de la información original (*input*) mediante un algoritmo matemático que transforma inputs en outputs de acuerdo a algún criterio, con la particularidad que es muy difícil recorrer el camino inverso, es decir, saber cuál fue el input que generó determinado output. Véase *supra* nota 76.

[98] Confr. Chris Coverdale, *A beginner's guide: private and public...o.c.*

[99] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en The Business Lawyer, Primavera 2019, p. 5.

[100] Idem, p. 6. Señalan que el PoW actual en Bitcoin y Ethereum cuesta aproximadamente 1 millón de Dólares diarios, entre energía eléctrica y hardware.

[101] Nathan Fulmer, *Exploring the legal...o.c.* p. 167.

[102] Aaron Wright y Primavera De Filippi, *Decentralized...p.* 13.

[103] Nathan Fulmer, *Exploring the legal...o.c.* p. 168.

[104] Ibid.

[105] Confr. Aaron Wright y Primavera De Filippi, *Decentralized...p.* 5.

[106] Puede ampliarse sobre el problema de los generales bizantinos en Leslie Lamport

et al., *The Byzantine Generals Problem*, ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS at 382 (July 1982), citado por Aaron Wright y Primavera De Filippi, *Decentralized...*p. 5, nota 16.

[107] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 501.

[108] Ibid.

[109] Ibid.

[110] Confr. Andrew Gazdecki, *Proof-Of-Work and Proof-Of-Stake: how blockchain reaches consensus*, recuperado el 05/04/2020 en <https://www.forbes.com/sites/forbestechcouncil/2019/01/28/proof-of-work-and-proof-of-stake-how-blockchain-reaches-consensus/#1f793d1568c8>.

[111] Ibid.

[112] Confr. HyperLedger, *HyperLedger Architecture*, Volume 1, recuperado el 05/04/2020 en <https://perma.cc/Y97U-8XGP>.

[113] PoET significa Proof Of Elapsed Time, y es un protocolo común en blockchains permissionadas o privadas. Su esencia es asignar a cada nodo la misma probabilidad de ser designado como ganador con derecho a proponer un bloque nuevo, y lo transmite al resto de los nodos para que lo validen y se incorpore así un bloque nuevo a la cadena preexistente.

[114] RBFT significa Redundant Byzantine Fault Tolerance. Ampliar en HyperLedger, *HyperLedger Architecture...* o.c., p. 7.

[115] Ampliar en Amy Castor, *A (short) guide to blockchain consensus protocols*, recuperado el 04/04/2020 de <https://www.coindesk.com/short-guide-blockchain-consensus-protocols>, quien enumera como otros ejemplos: Proof Of Activity, Proof Of Burn, Proof Of Capacity, y Proof Of Elapsed Time.

[116] Idem. Castor afirma que confirmar una nueva transacción -es decir, dar respuesta computacional al problema matemático asociado- se demora entre 10 y 60 minutos, y que la mayoría del poder de cómputo de minería está ubicado en países donde el costo de la energía es barato, ya que se requieren grandes cantidades de supercomputadoras. Esta respuesta que el minero debe encontrar para ganar el derecho a minar un bloque y generar bitcoins y comisiones, consiste en computacionalmente descubrir -mediante prueba y error, millones de veces- cuál combinación de datos produjo un *hash* determinado. Arvind Narayanan y otros, en *Bitcoin and cryptocurrency technologies*, recuperado el 10/04/2020 de https://www.lopp.net/pdf/princeton_bitcoin_book.pdf, p. 64, afirman que el PoW

funciona como un “*impuesto a la creación de identidades falsas en Bitcoin*”. Sin mucho poder cómputo, es poco probable que un minero “falso” llegue a minar un bloque. Señalan los autores que, para que un minero pueda crear un bloque nuevo, el minero que propone el bloque nuevo debe encontrar un número, llamado *nonce*, que cuando se concatena con (i) el *hash* anterior y con (ii) la lista de transacciones que compone el bloque y que forma el *hash* del bloque, produce un *target value*. La única forma de conseguir esto, es probar miles de *nonces*, hasta conseguir el *target value*. Una Mac Book no puede hacer este cálculo. A su vez, el *target value* que el minero debe encontrar es dinámico, y se ajusta al alza cada 2016 blocks, cuyo minado demanda usualmente dos semanas. En general, encontrar el *nonce* demora 10 minutos, y este período de tiempo se llama *latencia*. El *nonce* que cada minero encuentra se publica, y los demás mineros verifican que ese *nonce* está dentro del *target value*, y en consecuencia el minero que lo encontró, adquiere el derecho a minar el bloque nuevo. Otro concepto importante es el *hash power* o *hash rate*, que es la cantidad de intentos por segundo que un minero realiza para encontrar el *nonce* que le dará el derecho a minar un bloque. Para ampliar sobre el particular, se recomienda leer el artículo *Explaining hash rate or hash power in cryptocurrencies*, disponible al 12/04/2020 en <https://coinsutra.com/hash-rate-or-hash-power/>.

[117]

Ampliar en Arvind Narayanan y otros, en *Bitcoin and cryptocurrency...o.c.*, p. 62. La analogía del minero que extrae oro de la mina es adecuada para graficar el proceso retributivo de los nodos que agregan bloques a la blockchain de Bitcoin, proceso que, recuérdese, es capital-intensivo ya que se requiere un poder de cómputo importante, y mucha energía eléctrica. ¿Cuánto gana un minero por minar un bloque? Al 10 de Abril de 2020, un minero ganaba 12,5 bitcoins por cada bloque minado y agregado a la blockchain. El diseño particular de esta blockchain estipuló que la retribución del minero por cada bloque minado se fuera gradualmente reduciendo, a medida que se alcanzan hitos de 210.100 bloques. Este proceso es conocido como *Bitcoin Halving*. El primero ocurrió en 2012, el segundo en 2016, y el tercero ocurrió en Mayo de 2020, reduciendo la retribución de los mineros a 6,5 bitcoins por bloque. Más información sobre este proceso puede encontrarse en el siguiente link: <https://www.bitcoinblockhalf.com> disponible al 04/05/2020. Alyssa Hertig, en *Bitcoin halving, explained*, recuperado el 05/04/2020 de <https://www.coindesk.com/bitcoin-halving-explainer> afirma que con cada *halving*, la cantidad de bitcoins que se “emite”, i.e. se mina, se reduce a la mitad, con lo que si la demanda se mantiene, el precio del Bitcoin debiera subir ya que la oferta se reduce en un 50%. Esto es consecuencia de la reducción de la cantidad de bitcoins que reciben los mineros en pago por minar nuevos bloques, por lo que éstos tendrán menos cantidad para vender en el mercado a potenciales interesados, produciéndose una restricción de la oferta de bitcoins. En 2009, cuando Bitcoin empezó, cada 10 minutos se emitían 50 bitcoins en pago a los mineros. En 2019, cada 10 minutos se emiten 12,5 bitcoins en pago a los mineros.

como *black reward*, y a partir de Mayo de 2020, se emitirán sólo 6,25 bitcoins en pago a los mineros.

[118]

Confr. Arvind Narayanan y otros, en *Bitcoin and cryptocurrency...o.c.*, p. 63 sostiene que a medida que baje el *black reward*, subirán estas comisiones, que son determinadas por el minero según su libre criterio, existiendo algún nivel de competencia, especialmente en el canal mayorista, confr. <https://www.prnewswire.com/news-releases/bitcoin-sv-mining-fees-just-got-even-lower-coingeek-follows-taal-mining-with-fee-reductions-300983684.html>, recuperado al 05/04/2020. Desde el lanzamiento de Bitcoin en 2018 hasta Octubre de 2019, las comisiones por transacción de minado llegaron a 1 Billón de Dólares en total acumulado. Confr. <https://www.coindesk.com/bitcoin-just-hit-1-billion-in-all-time-transaction-fees> disponible al 08/04/2020.

[119]

Andrew Gazdecki, *Proof-Of-Work and Proof-Of-Stake...o.c.*

[120]

Obtenida en <https://perma.cc/9EQB-MA2W>.

[121]

Confr. American Chemical Society, *Estimating the environmental impact of Bitcoin mining*, recuperado el 06/04/2020 en <https://www.sciencedaily.com/releases/2019/11/191120080246.htm>.

[122]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 22.

[123]

Amy Castor, *A (short) guide...o.c.* sostiene que el validador debe invertir en la blockchain que usa PoS, adquiriendo las cryptomonedas que utilice.

[124]

Castor, o.c. sostiene que el validador que tenga 300 monedas, tendrá 3 veces más chances de ser elegido para validar una transacción que uno que tenga 100 monedas. Peercoin, <https://www.peercoin.net>, disponible al 05/04/2020 fue la primera criptomoneda en implementar PoS, y luego migró a un protocolo híbrido, con una moneda llamada NovaCoin, disponible al 04/05/2020 en <http://novacoin.org>. BlackCoin fue la segunda blockchain en usar PoS: <https://blackcoin.org> disponible al 05/04/2020.

[125]

Confr. Omar Faridi, en *Blockchain must guarantee immutability to remain competitive, Ethereum Classic developer says*, recuperado el 04/05/2020 de <https://www.cryptoglobe.com/latest/2018/10/blockchains-must-guarantee-immutability-to-remain-competitive-ethereum-classic-developer-says/>.

[126]

Confr. Pavel Vasin, *Blackcoin's Proof-Of-Stake Protocol v2*, disponible al 05/04/2020 en <https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdfv>.

[127] Confr. Daniel Won, *Date: Date + What you need to know*, disponible al 05/04/2020 en <https://www.exodus.io/blog/ethereum-proof-of-stake-date/>, quien sostiene que los validadores tienen distintos nombres según la blockchain de que se trate. Por ejemplo, se los llama *bakers* en la blockchain de Tezos, <https://tezos.com>, disponible al 05/04/2020.

[128] Confr. Casper, *the friendly GHOST of Ethereum*, recuperado el 06/04/2020 de <https://etherworld.co/2017/04/14/proof-of-stake-casper-the-friendly-ghost/>. Cada validador de Etheruem deberá depositar una cantidad de Ether en garantía, a modo de *escrow account*. Si Casper fuera desplegado, la posibilidad de ser validador de bloques pasará a depender proporcionalmente de la cantidad del depósito en garantía, y el monto mínimo de depósito sería ajustado dinámicamente.

[129] Confr., HyperLedger, *An introduction to HyperLedger*, p. 4, recuperado el 05/04/2020 en https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

[130] Confr. Kevin Werbach, *Bitcoin is gamification*, recuperado el 05/04/2020 en <https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22>.

[131] Confr. Andreas Antonopoulos, *Bitcoin security model: trust by computation*, recuperado el 06/04/2020 en <http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html>

[132] Confr. Reid Hoffman, *Why blockchain matters*, entrevista disponible al 06/04/2020 en <https://www.wired.co.uk/article/bitcoin-reid-hoffman>.

[133] Confr. Andreas Antonopoulos, *Bitcoin security model...o.c.*

[134] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 501, nota 66.

[135] Ibid.

[136] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 548.

[137] El Bitcoin Core puede descargarse, al 16/04/2020, en <https://bitcoin.org/en/download>.

[138] El BIP 9 permite que los mineros manden “señales” cuando están listos para implementar nuevas reglas. Ampliar en Kile Torpey, *BIP 9: Enabling easier changes and upgrades to Bitcoin*, disponible al 12/04/2020 en <https://bitcoinmagazine.com/articles/bip-enabling-easier-changes-and-upgrades-to-bitcoin-1453929816>.

[139] Ampliar en <https://steemit.com/spanish/@tunetworker/que-es-el-bip-91-de-que-sirve-y-lo-que-no-hace-con-el-bitcoin>, recuperado el 16/04/2020.

[140] SegWit es el acrónimo de la tecnología conocida como *Segregated Witness*, diseñada para aumentar la velocidad y eficiencia de las transacciones de Bitcoin y reducir su volumen. SegWit ha sido adoptado por un 66% de los mineros, a Enero de 2020. Confr. William Suberg, *La adopción de SegWit de la red Bitcoin llega al 66% después que BitMEX admitiera dicha actualización*, recuperado el 15/04/2020 en <https://es.cointelegraph.com/news/bitcoin-network-segwit-adoption-hits-66-after-bitmex-embraces-upgrade>.

[141] Ampliar en <https://www.coindesk.com/coindesk-explainer-bitcoin-bip-91-implements-segwit-avoiding-split>, recuperado el 16/04/2020.

[142] Confr. Binance, *A beginner's guide to Segregated Witness (SegWit)*, recuperado el 15/04/2020 en <https://www.binance.vision/blockchain/a-beginners-guide-to-segretated-witness-segwit>.

[143] Ibid.

[144] Me refiero al período histórico que algunos llamaron *CryptoWinter*. Ampliar en el muy interesante artículo de Julia Magas, *Ethereum Ice Age may be imminent if miners withdraw from network*, recuperado al 10/04/2020 en <https://cointelegraph.com/news/ethereum-ice-age-may-be-imminent-if-miners-withdraw-from-network>

[145] Cada vez que se habla de la blockchain pública de Ethereum, debe tenerse siempre presente que utilizar esta blockchain, implica pagar por su uso en *gas*. Debido al alto costo que insume ejecutar programas descentralizados como las Dapps, y a la necesidad de evitar o minimizar el riesgo de ser objeto de un ataque de tipo *Denial Of Service* (DoS), Ethereum utiliza un recurso contable llamado *gas*, con el que se paga por usar la blockchain de Ethereum. Para que una Dapp en Ethereum pueda funcionar –e.g. un smart contract–, siempre deberá tener *gas* en su cuenta, o no podrá usar esta blockchain. El *gas*, entonces, mide el esfuerzo computacional que debe hacerse para ejecutar ciertas acciones en la blockchain de Ethereum. Cualquier acción en la blockchain de Ethereum, consume alguna cantidad de *gas*. A los mineros de Ethereum se les paga por sus trabajos, para incentivarlos –así como en Bitcoin se pagan *block rewards*– en una proporción equivalente a todo el *gas* que hayan consumido para realizar la operación de que se trate, es decir, las comisiones de los mineros que hacen correr un smart contract en la blockchain de Ethereum, se pagan en *gas*, que uno debe previamente adquirir o comprar al minero. El precio “testigo” del *gas* se calcula para una orden de trabajo “promedio” de 20 Gweis; una unidad de Gwei equivale a

0.0000000001 Ethers –es decir, 1 Gwei es la billonésima parte de 1 Ether–; al 16/04/2020 1 Ether vale a U\$D 170,27, con lo cual un Gwei cuesta 0,000000017 U\$d, y 20 Gwei equivalen a 0,00000034 U\$D. Cada tramo de un smart contract tiene una transacción programada, y cada transacción consume una determinada cantidad gas, con lo cual uno puede saber de antemano cuánto le gas le costará hacer correr su contrato inteligente, ya que, en síntesis, cada línea de programación en el lenguaje Solidity que es el que usa la Ethereum Virtual Machien (EVM) consume indefectiblemente gas. El precio del gas es variable, y puede consultarse aquí: <https://ethgasstation.info>. Existen además mercados donde uno puede vender, o comprar gas, confr. <https://www.cryptoground.com/gas-exchanges>. Ampliar en Ameer Rosic, *What is Ethereum gas? (the most comprehensive step-by-step guide ever!)*, disponible al 16/04/2020 en <https://blockgeeks.com/guides/ethereum-gas/>; en Joseph Chow, *Ethereum, Gas, Fuel & Fees*, video explicativo disponible al 16/04/2020 en <https://www.youtube.com/watch?v=dd-ajiMl4HY>; y en Danny Ryan, *Costs of a real world Ethereum contract*, disponible al 17/04/2020 en <https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214>.

Ari Juels, Ahmed Kosba y Elaine Shi, en *The ring of Gyges: investigating the future of Criminal Smart Contracts*, recuperado el 17/04/2020 en https://www.researchgate.net/publication/310821111_The_Ring_of_Gyges_Investigati definen el gas como una forma de comisión por transacción, que es proporcional al tiempo de ejecución del contrato.

[146] Véase *infra* en § 2.7.1.1, una descripción completa del caso.

[147] Confr. Alice Lloyd George, *Behind the scenes with Tezos, a new blockchain upstart*, recuperado el 13/04/2020 en <https://techcrunch.com/2017/07/12/behind-the-scenes-with-tezos-a-new-blockchain-upstart/>.

[148] Ibid.

[149] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 550.

[150] Confr. Gideon Greenspan, *The blockchain immutability myth*, recuperado el 16/04/2020 en <https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/>.

[151] Ibid.

[152] HyperLedger, confr. <https://en.wikipedia.org/wiki/Hyperledger>, recuperado al 18/04/2020.

[153] Véase *infra* en 3.5.1.10.

[154] Confr. Accenture, *Why distributed ledger technology must adapt to an imperfect*

world, recuperado el 18/04/2020 en https://www.accenture.com/t00010101T000000_w/es-es/acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf.

[155] Ampliar en Carlos Cortés, *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital*, recuperado al 18/04/2020 en <https://www.palermo.edu/cele/pdf/DerechoalolvidoiLEI.pdf>; véase también el informe especial del Parlamento Europeo, *Blockchain and the General Data Protection Regulation*, recuperado al 18/04/2020 en [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)0010_en.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)0010_en.pdf) y IBM White Paper, *Blockchain and GDPR*, recuperado al 15/04/2020 en <https://iapp.org/resources/article/blockchain-and-gdpr/>.

[156] Confr. Gideon Greenspan, *The blockchain immutability ...o.c.*

[157] Confr. Nikolaos Kostopoulos, en *The battle between private and public blockchains*, recuperado el 19/04/2020 en <https://hackernoon.com/the-battle-between-private-and-public-blockchains-b01a35rb>.

[158] Confr. Thibault Schrepel, en *Collusion by Blockchain and...o.c.* p. 31.

[159] Ibid.

[160] Confr. Kevin Werbach, en *Trust, but verify... o.c.* p. 511.

[161] Kevin Werbach, en *Trust...o.c.* p. 503 sostiene que si bien los usuarios están identificados por una especie de firma digital, eso no necesariamente permite conocer la identidad real detrás de esa llave pública. Incluso, si una transacción se parte en cientos de pequeñas transacciones, se pueden camuflar grandes transferencias de monedas digitales sin saber quién es el beneficiario último.

[162] Confr., Marc Pilkington, en *Blockchain technology: principles..o.c.* Curiosamente, las dos blockchains públicas más populares han sido modificadas por distintas causas pero con un mismo objetivo: garantizar su operabilidad y mejorar funcionamiento, con lo cual luce controvertido el atributo de *inmutabilidad*. Pilkington incluso señala que Buterin mismo reconoce la necesidad de poder modificar el registro de la blockchain en ciertas condiciones, principalmente cuando el gobierno es parte de la blockchain.

[163] Para entender el funcionamiento de Bitcoin, es recomendable remitirse directamente a la fuente: Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash sistem*, recuperado al 03/04/2020 en <https://bitcoin.org/bitcoin.pdf>.

[164] Al igual que en el caso de Bitcoin, para entender el funcionamiento de

Ethereum, es recomendable remitirse directamente a la fuente: Vitalik Buterin, *A next-generation smart contract and decentralized application platform*, recuperado el 03/04/2020 en <https://github.com/ethereum/wiki/wiki/White-Paper>.

[165] Confr. https://es.wikipedia.org/wiki/Vitalik_Buterin, recuperado al 20/04/2020.

[166] Confr. Genny Diaz, en *Ethereum: historia de la plataforma de contratos inteligentes más usada*, recuperado el 10/04/2020 de <https://www.criptonoticias.com/redes-protocolos/ethereum-historia-plataforma-contratos-inteligentes-usada/>.

[167] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 22.

[168] Véase *supra* [nota 145](#) para una descripción de cómo funciona este interesante sistema de “pay-per-use” de Ethereum.

[169] Ibid.

[170] Confr. <https://nomics.com/assets/eth-ethereum>, recuperado al 14/04/2020.

[171] Confr. <https://entethalliance.org/enterprise-ethereum-alliance-launches/>.

[172] Confr. <https://entethalliance.org/members/>.

[173] Vlad Zamfir, en *About my tweet from yesterday*, recuperado el 14/04/2020 en https://medium.com/@Vlad_Zamfir/about-my-tweet-from-yesterday-dcc61915b572.

[174] Ibid.

[175] Véase <https://sovrin.org>

[176] Ampliar en Angela Walch, *The bitcoin blockchain as financial market infrastructure: a consideration of operational risk*, disponible el 16/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482.

[177] Angela Walch, *The bitcoin blockchain ...* p. 875, define al software *open source* como aquél que hace público su código fuente, libremente accesible al mundo, pudiendo los usuarios modificarlo, alterarlo, mejorarlo. Lo opuesto es el software *propietario*, donde la licencia de uso generalmente prohíbe modificar su código fuente. El software de código abierto es desarrollado de modo colaborativo y abierto. Siendo Bitcoin un software *open source*, no hay nadie formalmente encargado de mantenerlo, actualizarlo y corregirlo. Esto produce que existan demoras en efectuar correcciones a fallas detectadas. Además, los cambios propuestos para reparar cualquier malfuncionamiento, deben ser voluntariamente aceptados por todos los nodos, de lo

contrario se dividirá la cadena entre aquellos que actualicen la última versión, y aquellos otros que no lo hagan. Un ejemplo de esto, es la discusión sobre el tamaño del bloque. Amplair en Remitano, *Bitcoin block size: why there's a 1MB limit*, recuperado al 14/04/2020 en <https://remitano.com/forum/ar/post/139-bitcoin-block-size-why-theres-a-1mb-limit>. Véase también notas 213, 408.

[178] Angela Walch, *The bitcoin blockchain ...o.c.*, p. 845.

[179] En GitHub, al 14/04/2020 se listan 780 *issues* sin resolución, es decir, *bugs*. Confr. <https://github.com/bitcoin/bitcoin/issues>.

[180] Los ataques deben dividirse entre: (i) ataques al software de Bitcoin y su plataforma operativa *per se*, y (ii) ataques a intermediarios, i.e. empresas que prestan servicios a los usuarios de la plataforma de Bitcoin, tales como exchanges (e.g. Coinbase, BitStamp, OKCoin), wallets (Circle, Armory, DarkWallet), y procesadores de pago (BitPay, Coin.co). Muchas de éstas empresas intermediarias han sufrido ataques intentando robar las bitcoins que tienen en depósito, pero esos ataques no son ataques al software de Bitcoin *per se*. Se ha sostenido que el software de Bitcoin es probablemente el más seguro del mundo, y para ser hackeado sería necesario muchísimo poder de cómputo. Confr. Angela Walch, *The bitcoin blockchain ...o.c.*, p. 860, nota 109

[181] El software de Bitcoin Core, a Abril de 2020, va por la actualización número 70 (!). Confr. *Bitcoin Core version history*, en <https://bitcoin.org/en/version-history>. El problema no son las actualizaciones, que en todo caso resuelven problemas del código, sino que las actualizaciones no sean instaladas por todos los nodos. En 2015, Bitcoin sufrió un *hard fork* que produjo, temporariamente, que existieran dos cadenas de bloques distintas, confr. Angela Walch, *The bitcoin blockchain ...o.c.*, p. 866. En la historia de Bitcoin, ha habido muchos *hard forks*, que han dado nacimiento a nuevas monedas, que se desprendieron del código original de Bitcoin. Para un análisis de las principales monedas, especie de obras derivativas de Bitcoin, consultar en BitDegree, *Bitcoin forks: history and upcoming Bitcoin forks*, disponible al 14/04/2020 en <https://www.bitdegree.org/tutorials/bitcoin-fork/>.

[182] Angela Walch, *The bitcoin blockchain ...o.c.*, p. 856.

[183] Confr. Ittal Eyal y Emin Gün Sirer, *Majority is not enough: Bitcoin mining is vulnerable*, recuperado el 14/04/2020 en <https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf>.

[184] Confr. Vitalik Buterin, en *DAOs, DACs, DAs and more: an incomplete terminology guide*, recuperado el 15/04/2020 en <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide>.

[terminology-guide/](#). Ampliar en Vitalik Buterin, *Bitcoin network shaken by blockchain fork*, recuperado el 15/04/2020 en <https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448>.

[185] Confr. Jordan Tuwiner, *Bitcoin mining pools*, recuperado al 14/04/2020 en <https://www.buybitcoinworldwide.com/mining/pools/>.

[186] Ibid.

[187] Ibid.

[188] Angela Walch, *The bitcoin blockchain ...o.c.*, p. 863.

[189] Confr. Johann Polecsak, *Will Google's Quantum Supremacy break Bitcoin in 2020?* Recuperado el 14/04/2020 en <https://cointelegraph.com/news/will-googles-quantum-supremacy-break-bitcoin-in-2020>.

[190] Confr. Bill Holtz, *Quantum-resistant cryptography: our best defense against an impending Quantum apocalypse*, recuperado el 14/04/2020 en <https://www.forbes.com/sites/forbestechcouncil/2019/09/25/quantum-resistant-cryptography-our-best-defense-against-an-impending-quantum-apocalypse/#1fada7941279>.

[191] Confr. Ian Bogost, *Cryptocurrency might be a path to Authoritarianism*, recuperado el 15/04/2020 en <https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/>.

[192] Confr. Trent Lapinski, *Will blockchain technology be used to build evil social credit systems?*, recuperado el 15/04/2020 en <https://cointelegraph.com/news/will-blockchain-technology-be-used-to-build-evil-social-credit-systems>.

[193] Confr. <https://cointelegraph.com/news/chinas-total-blockchain-investments-dropped-40-in-2019-compared-to-2018>, recuperado el 15/04/2020. Sólo en 2019 –con un volumen de inversión 40% menor a 2018, China fundó 3.5 billones de dólares en empresas, proyectos y consolidaciones vinculadas al blockchain. Confr. <https://www.dcfcasts.com/blockchain-news/chinese-blockchain-startups-got-3-5-billion-in-2019/>

[194] Confr. Trent Lapinski, *Will blockchain technology be used to build...o.c.*

[195] Disponible al 15/04/2020 en <http://www.caict.ac.cn/english/yjcg/bps/201901/P020190131402018699770.pdf>.

[196] Confr. Arjun Kharpal, *With Xi's backing, China looks to become a world leader in*

blockchain as US policy is absent, recuperado el 14/05/2020 en <https://www.cnn.com/2019/12/16/china-looks-to-become-blockchain-world-leader-with-xi-jinping-backing.html>.

[197] Ibid.

[198] Confr. Thibault Schrepel, en *Collusion by Blockchain and...* o.c. p. 32.

[199] Confr., Marc Pilkington, en *Blockchain technology: principles...* o.c.

[200] Confr., Coindesk, *What is the difference between public and permissioned blockchains?*, recuperado el 15/04/2020 en <https://perma.cc/A8E4-EE4N>.

[201] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 514.

[202] Confr. Thibault Schrepel, *Is blockchain the death of antitrust law? The blockchain antitrust paradox*, publicado en *Georgetown Law Technology Review*, Vol. 3.2, número 281, 2019, p. 290.

[203] Confr., Renato Mangano, *Blockchain securities, insolvency law and the sandbox approach*, publicado en *European Business Organization Law Review*, (2018), número 19, p. 715. Thibault Schrepel, *Is blockchain the death...* o.c., p. 290 sostiene que en estas blockchains privadas consorciadas el proceso de consenso es controlado por un grupo pre-determinado de nodos, e.g., el consenso podría operar con 5 empresas, cada uno de las cuales opera un nodo, y para validar un bloque nuevo, 3 de las 5 deben aceptarlo. La característica determinante es que las blockchains consorciadas son dirigidas por un grupo de entidades, y no por una sola entidad. Schrepel también sostiene que existe una categoría de blockchains semi-privadas, a las que se denomina *híbridas* en este Manual.

[204] Véase <https://www.goquorum.com>

[205] Véase <https://www.tradelens.com>

[206] Véase <https://gandal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/>

[207] Confr. <https://es.cointelegraph.com/news/walmart-to-implement-blockchain-based-delivery-system>, recuperado al 03/05/2020. Ampliar en Matthew Spoke, *Private blockchains were a good start: but they are not the future*, <https://www.forbes.com/sites/mattspoke/2019/08/27/private-blockchains-were-a-good-start-but-they-are-not-the-future/#42fe49676cd7> disponible al 05/05/2020.

[208] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 498. Para una idea de costos de implementación de una blockchain privada, véase EY, *total cost of ownership for*

blockchain solutions, disponible al 05/05/2020 en [https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/\\$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf](https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf).

[209] Confr. <https://www.hyperledger.org>

[210] Ampliar en: <https://docs.google.com/presentation/d/1yApb74bhpdXusfz2JmOwOVtlPeqhMCBvJV> disponible al 14/05/2020.

[211] Véase *infra* en § 1.3.3.

[212] Confr. Richard Gendal Brown, *Towards deeper collaboration in distributed ledgers: thoughts on digital asset's global synchronisation log*, recuperado el 15/04/2020 en <https://gendal.me/2017/01/24/towards-deeper-collaboration-in-distributed-ledgers-thoughts-on-digital-assets-global-synchronisation-log/>.

[213] Ibid. Y se requiere pensar formas de ampliar la “capacidad del sistema”. Para una revisión de los argumentos involucrados en la discusión del tamaño del bloque en Bitcoin, véase <https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit>, recuperado el 14/04/2020.

[214] Confr. Konstantinos Christidis y Michael Devetsikiotis, en *Blockchains and Smart Contracts for the Internet of Things*, recuperado el 20/04/2020 en <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408>, p. 2297.

[215] Confr. <https://www.multichain.com/developers/permissions-management/>, recuperado el 22/04/2020.

[216] Véase también *infra* notas 413 y 445. Konstantinos Christidis y Michael Devetsikiotis, o.c., p. 2295 explican con mucha claridad cómo funciona este mecanismo en Bitcoin: “*the validation checks that we would encode into the nodes of a blockchain network that is set up for such asset transfers would be: Does the proposed transaction address (use) an existing row? Is it properly signed so as to delete that row (or rows)? Has this row been addressed (used) by a previous validated transaction? An asset cannot be spent twice. Does it transfer the right amounts to new rows? For example, if the row transaction reads “10 units of X”, an attempted transfer of “2 units of X” (to Bob) and “9 units of X” (back to Alice) should fail. Same goes for an attempted transfer of, say, “10 units of Y”. The sum of inputs should equal the sum of outputs, i.e. a transfer should not increase the total quantity of an asset type. Note that a transaction can address several existing rows instead of just one, i.e. transfer assets scattered over the database, as long as it is properly signed to access them. These existing, not-yet-deleted rows are called unspent transaction outputs (UTXO) in*

Bitcoin; they were created by earlier transactions in the system. The UTXO that a transaction consumes are called transaction inputs; the UTXO that a transaction creates are called transaction outputs. **A transaction then basically deletes a set of rows (UTXO) and creates a set of new rows (UTXO) in the database (...)** how do we generate assets and introduce them in the chain? Before we get to the state of Alice having 10 units of X, these 10 units of X have to come from somewhere. **In the case of Bitcoin, new bitcoins are introduced into the network with every mined block:** The mining node includes a so-called coinbase transaction in the block of transactions it broadcasts to the network. **This coinbase transaction has no inputs and rewards the mining node with a pre-determined (by the network) amount of bitcoins.**

The key thing to keep in mind is this: **if you have a set of users (a) who want to trade digital tokens, and (b) have agreed on how these tokens are generated, then a blockchain network is an ideal tool to use both for exchanging these tokens, and tracking who has what. No middleman is needed to facilitate the exchanges cause every node on the network runs the the necessary checks and reaches consensus on the accepted result.** Asset tracking comes out-of-the-box since every node has access to the agreed set of cryptographically verifiable transactions on the blockchain.” De lo expuesto surge que la blockchain es un “method for **tagging different pieces of information as belonging to different participants, and enforcing this form of data ownership without a central authority.**” Los resaltados son míos.

Puede ampliarse también en UTXO, <https://medium.com/@Consensys/thoughts-on-utxo-by-vitalik-buterin-2bb782c67e53>, recuperado el 22/04/2020.

[217]

Ampliar en Flora Sun, *UTXO vs. Account/Balance Model*, recuperado el 24/04/2020 en <https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf>. Sun afirma en relación a UTXO: “A user’s wallet keeps track of a list of unspent transactions associated with all addresses owned by the user, and **the balance of the wallet is calculated as the sum of those unspent transactions.**” Lo ejemplifica así: “1. Alice gains 12.5 bitcoins through mining. Alice’s wallet is associated with one UTXO record of 12.5 bitcoins. 2. Alice wants to give Bob 1 bitcoin. Alice’s wallet first unlocks her UTXO of 12.5 bitcoins and uses this whole 12.5 bitcoins as input to the transaction. This transaction sends 1 bitcoin to Bob’s address and the remainder of 11.5 bitcoins is sent back to Alice in the form of a new UTXO to a newly-created address (owned by Alice). 3. Say there was another UTXO of 2 bitcoins associated with Bob prior to step 2, Bob’s wallet now shows that his balance is 3 bitcoins. **Bob’s wallet now keeps track of two UTXOs: one from before and another from the transaction in step 2.** Each UTXO needs to be unlocked if Bob wishes to spend them.” El otro modelo, en cambio, “**keeps track of the balance of each account as a global state.** The balance of an account is checked to make sure it is larger than or equal to the spending transaction amount. Here is a simplified example of how this model works in Ethereum: 1. Alice gains 5 ethers through mining. It is recorded in the system that Alice has 5 ethers. 2. Alice wants to give

Bob 1 ether, so the system will first deduct 1 ether from Alice's account, so Alice now has 4 ethers.³ The system then increases Bob's account by 1 ether. The system knows that Bob has 2 ethers to begin with, therefore Bob's balance is increased to 3 ethers. (...) the record-keeping for Ethereum **is just like that in a bank**. An analogy is using an ATM/debit card. The bank tracks how much money each debit card has, and when we need to spend money, the bank checks its record to make sure we have enough balance before approving the transaction." El resaltado es mío.

[218]

Confr. Thibault Schrepel, *Is blockchain the death of antitrust law?...o.c.*, p. 295.

[219]

En 2014, Vitalik Buterin daba una definición de las Dapps en un artículo titulado *DAOs, DACs, DAs and more: an incomplete terminology guide*, recuperado el 15/04/2020 en <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>. Una Dapp –*decentralized application*– es variación de un Smart Contract, es decir un mecanismo que involucra activos digitales y dos o más partes, donde alguna o todas las partes afectan activos digitales, los que son automáticamente distribuidos entre las partes de acuerdo a una fórmula basado en ciertos datos que, al momento de iniciar el contrato, no son conocidos. La Dapp es similar a un smart contract, pero con dos diferencias: (i) puede haber un número ilimitado de participantes de cada lado del contrato y (ii) no tiene necesariamente que estar vinculada a transacciones financieras. Las Dapps son divididas a su vez en dos clases: (a) totalmente anónimas, o (b) basadas en reputación, a donde algunos nodos siguen la performance de otros, con el fin de mantener la confianza en ellos.

[220]

Idem. Buterin define a las DOs –*decentralized organizations*– como una organización en la que los humanos participan de acuerdo a las reglas fijadas en el protocolo programado –como si fuera el Estatuto Social de una sociedad anónima, o el Estatuto Social de una asociación civil–, pero aplicado a raja tabla por la blockchain. Toda la estructura convencional de las sociedades y su tipología legal y tipos de organicismo, puede ser migrado a una blockchain, para que registre las tenencias de los accionistas, quienes expresan su voluntad –votan– también vía blockchain. Lo mismo es predicable respecto de personas jurídicas sin fines de lucro. Una DO puede controlar activos digitales, o físicos, en la medida que su código interactúe con tales activos.

[221]

Idem. Buterin define a las DAOs –*decentralized autonomous organizations*– como el Santo Grial. Una DAO es un término genérico, que incluye también las DACs –*decentralized autonomous corporations*–, una especie de DAO. A diferencia de las DOs, las DAOs y DACs son entidades que viven en Internet, son autónomas, y pueden contratar a personas para que realicen las tareas que ellas no pueden. Las DAOs vendrían a emular a una fundación o asociación civil, entidades sin fines de lucro, aunque tienen un *capital social digital*, y están facultadas por su código de

programación para disponer de dicho capital en ciertas circunstancias, generalmente para retribuir o premiar conductas. Las DOs también tienen un capital, pero está gestado por humanos que son quienes toman las decisiones; mientras que el capital de las DAOs está gestado por el código de la DAOs, de manera autónoma.

[222] Véase el artículo de Ying-Yeng Hsieh, Jean-Philippe Vergne, Philip Anderson, Karim Lakhani y Markus Reitzig, *Bitcoin and the rise of decentralized autonomous organizations*, recuperado el 15/04/2020 de <https://link.springer.com/content/pdf/10.1186/s41469-018-0038-1.pdf>. Sostienen los autores citados que Bitcoin es el primer DAO en la historia del diseño de las organizaciones.

[223] Idem. Buterin define a las DACs como una especie de DAOs, con la diferencia que la DAC paga dividendos, es decir, es una persona jurídica digital con fines de lucro, a diferencia de las DAOs que son sin fines de lucro. Buterin señala que el énfasis en los dividendos puede complicar definir situaciones en las que los partícipes reciben *tokens* como dividendos, y estos *tokens*, a su vez, pueden ser (i) “permisos de uso” de ciertos activos digitales que integran “el activo” de la DAO o de la DAC, o pueden ser (ii) monedas propias emitidas por la DAO/DAC, o pueden (iii) ser otras criptomonedas adquiridas en contraprestación por los bienes y servicios producidos por la DAO/DAC y comercializados a terceros, o (iv) moneda fiat, de curso legal, convencional, emitida por un Estado.

[224] Cuando un sistema computable combina Dapps, DAOs o DACs, estamos frente a un *Decentralized Autonomous System*, o DAS.

[225] Confr. Kalliopi Kyriotaki, Efpraxia Zamani y George Giaglis, en *From Bitcoin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-peer networks and blockchains*, disponible al 15/04/2020 en <https://www.researchgate.net/publication/283020776> [From Bitcoin to Decentralized Peer-to-Peer Networks and Blockchains](https://www.researchgate.net/publication/283020776).

[226] Ibid.

[227] Ibid.

[228] Confr. Ellie Zolfagharifard, *Would you take orders from a robot? An artificial intelligence becomes the world's first Company director*, recuperado el 14/05/2020 en <https://www.dailymail.co.uk/sciencetech/article-2632920/Would-orders-ROBOT-Artificial-intelligence-world-s-company-director-Japan.html>.

[229] Ibid.

- [230] Confr., Gartner, Inc., *The real business of blockchain*,... p.10.
- [231] Confr. <https://alastria.io/asociacion/>.
- [232] Ibid.
- [233] Confr. <https://www.eublockchainforum.eu>. Ampliar en European Court of Auditors, *The European Blockchain Services Infrastructure is coming, and the ECA has a role to play*, recuperado el 15/04/2020 en <https://medium.com/ecajournal/the-european-blockchain-services-infrastructure-is-coming-and-the-eca-has-a-role-to-play-68b53395c788>.
- [234] Confr. <https://www.ico.li/liechtenstein-eu-partnership/>
- [235] Confr. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>
- [236] Véase *infra* en § 3.5.1.10.3.
- [237] Ibid.
- [238] Confr. <https://inatba.org/imprint/>.
- [239] Confr. <https://www.blockadvocacy.org/press>.
- [240] Confr. <https://www.ledgerinsights.com/iso-blockchain-standards/>.
- [241] Confr. <https://www.bitcoinargentina.org>.
- [242] Véase *infra* en § 3.5.1.4.
- [243] Confr. <https://bfa.ar/bfa/infraestructura>.
- [244] Confr. *Deloitte's 2019 Global blockchain survey*, recuperada el 15/04/2020 en https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf, p. 3.
- [245] Confr. Maximilian Friedlmaier, Andranik Tumasjan y Isabell Welpé, en *Disrupting industries with blockchain: the industry, the venture capital funding, and regional distribution of blockchain ventures*, recuperado el 14/04/2020 en <https://pdfs.semanticscholar.org/c6a6/6e8a80c7174c7bd7a227f81c7c7ecffce17d.pdf>.
- [246] Nathan Fulmer, *Exploring the legal...* o.c. p. 189.
- [247] Véase *supra* en 1.1.9.1.1.
- [248] Confr. Patrick Murck, *Quién controla la cadena de bloques?* en Harvard Business

Review, 19/04/2017, recuperado el 15/04/2020 en <https://hbr.org/2017/04/who-controls-the-blockchain>.

[249]

Confr. Jason Bloomberg, *Eight reasons to be skeptical about blockchain*, recuperado el 14/04/2020 en <https://perma.cc/9H58-FNZ9>, citado por Nathan Fulmer, *Exploring the legal...* o.c. p. 190.

[250]

Para un análisis de los hard forks en Bitcon, véase Nathan Reiff, *A history of Bitcoin hard forks*, recuperado el 14/04/2020 de <https://www.investopedia.com/tech/history-bitcoin-hard-forks/>.

[251]

Véase *supra* nota 180. Véase también el interesante artículo de Jon Matonis, *The Bitcoin mining arms race: GHash.io and the 51% issue*, recuperado el 15/04/2020 en <https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue>.

[252]

Véase *supra* nota 176.

[253]

Confr. MIT Technology Review, *First quantum-secured blockchain technology tested in Moscow*, recuperado el 14/05/2020 <https://www.technologyreview.com/2017/06/06/151368/first-quantum-secured-blockchain-technology-tested-in-moscow/>.

[254]

Confr. *How the crypto world is preparing for Quantum computing, explained*, recuperado el 14/05/2020 en <https://cointelegraph.com/explained/how-the-crypto-world-is-preparing-for-quantum-computing-explained>.

[255]

Confr. Jacob Ramirez, *Bitcoin in the age of Quantum computing*, recuperado el 15/05/2020 en <https://hackernoon.com/bitcoin-in-the-age-of-quantum-computing-czg633u5>.

[256]

Confr. Daniel Kraus y Charlotte Boulay, *Blockchains: aspects of Intellectual Property Law*, p. 17, recuperado el 14/05/2020 en https://www.researchgate.net/publication/332641100_Blockchains_Smart_Contracts_I

[257]

Confr. Anca F., *Bitcoin price prediction and analysis in April 2020. Is BTC affected by coronavirus?* Disponible al 16/04/2020 en <https://coindoo.com/bitcoin-price-prediction-april/>.

[258]

Se recomienda visitar el MIT CryptoEconomics Lab para profundizar sobre la (muy apasionante) temática: <https://ce.mit.edu>.

[259]

Confr. Huobi Research, *Theoretical foundation of Token Economics in Nobel Prize in Economic Science*, recuperado el 16/04/2020 en <https://medium.com/huobi-research/theoretical-foundation-of-token-economics-in-nobel-prize-in-economic>

[science-2853570e3cc6](https://doi.org/10.1007/s40804-018-0123-5).

[260]

Confr. Renato Mangano, *Blockchain securities, insolvency law and the sandbox approach*, publicado en *European Business Organization Law Review*, (2018) 19, p. 715–735, disponible al 16/04/2020 en <https://doi.org/10.1007/s40804-018-0123-5>.

[261]

La Ley de Mercado de Capitales N° 26.831, modificada por la Ley de Financiamiento Productivo N° 27.440, en su Art. 2 define a los *Valores Negociables* como títulos valores emitidos tanto en forma cartular así como a todos aquellos valores incorporados a un registro de anotaciones en cuenta incluyendo, en particular, los valores de crédito o representativos de derechos creditorios, las acciones, las cuotas partes de fondos comunes de inversión, los títulos de deuda o certificados de participación de fideicomisos financieros o de otros vehículos de inversión colectiva y, en general, cualquier valor o contrato de inversión o derechos de crédito homogéneos y fungibles, emitidos o agrupados en serie y negociables en igual forma y con efectos similares a los títulos valores; que por su configuración y régimen de transmisión sean susceptibles de tráfico generalizado e impersonal en los mercados financieros. Asimismo, quedan comprendidos dentro de este concepto, los contratos de futuros, los contratos de opciones y los contratos de derivados en general que se registren conforme la reglamentación de la Comisión Nacional de Valores, y los cheques de pago diferido, certificados de depósitos de plazo fijo admisibles, facturas de crédito, certificados de depósito y warrants, pagarés, letras de cambio, letras hipotecarias y todos aquellos títulos susceptibles de negociación secundaria en mercados.

[262]

El Código Civil y Comercial de la Nación (CCCN) los define en su Art. 1815 como aquellos que incorporan una obligación incondicional e irrevocable de una prestación y otorgan a cada titular un derecho autónomo. El Art. 1820 CCCN a su turno dispone que cualquier persona puede crear y emitir títulos valores en los tipos y condiciones que elija. Se comprende en esta facultad la denominación del tipo o clase de título, su forma de circulación con arreglo a las leyes generales, sus garantías, rescates, plazos, su calidad de convertible o no en otra clase de título, derechos de los terceros titulares y demás regulaciones que hacen a la configuración de los derechos de las partes interesadas, que deben expresarse con claridad y no prestarse a confusión con el tipo, denominación y condiciones de los títulos valores especialmente previstos en la legislación vigente. Sólo pueden emitirse títulos valores abstractos no regulados por la ley cuando se destinan a ofertas públicas, con el cumplimiento de los recaudos de la legislación específica; y también cuando los emisores son entidades financieras, de seguros o fiduciarios financieros registrados ante el organismo de contralor de los mercados de valores. El Art. 1836 CCCN, por su parte, dispone que los títulos valores tipificados legalmente como cartulares también pueden emitirse como no cartulares, para su ingreso y circulación en una caja de valores o un sistema autorizado de compensación bancaria o de anotaciones en cuenta. Los títulos valores emitidos

efectivamente como cartulares pueden ingresarse a alguno de estos sistemas, conforme con sus reglamentos, momento a partir del cual las transferencias, gravámenes reales o personales y pago tienen efecto o se cumplen por las anotaciones en cuenta pertinentes.

[263] Confr. Renato Mangano, *Blockchain securities, insolvency ...o.c.*, p. 717.

[264] Ibid.

[265] Confr. <https://coinmarketcap.com/es/exchanges/cryptomarket/>. Para ver la evolución de las principales monedas digitales en 2019, puede consultarse el artículo de Julia Magas, *Biggest crypto price movements in 2019*, recuperado el 16/04/2020 en <https://coingecko.com/news/biggest-crypto-price-movements-of-2019>.

[266] Confr. <https://coinmarketcap.com/charts/>, disponible al 16/04/2020.

[267] Argentina no fue la excepción, sancionado el 27 de Diciembre de 2017 la Ley 27.430 (B.O. 29/12/2017), que en su Art. 2, dispuso someter al Impuesto a las Ganancias los resultados obtenidos derivados de la enajenación de monedas digitales, cualquiera sea el sujeto que las obtenga. Ampliar en el artículo de Martina Caunedo, *Una abogada experta en criptomonedas explica qué impuestos hay que pagar en la Argentina*, recuperado el 16/04/2020 en <https://www.infobae.com/cripto247/altcoins/2018/07/20/una-abogada-experta-en-criptomonedas-explica-que-impuestos-hay-que-pagar-en-la-argentina/>.

[268] Confr. <https://www.bankofengland.co.uk/news/2020/january/central-banks-group-to-assess-digital-currencies>, recuperado al 16/04/2020.

[269] Confr. <https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency>, recuperado el 16/04/2020.

[270] Confr. <https://www.cripto247.com/comunidad-cripto/el-fmi-analiza-ventajas-y-desventajas-de-las-monedas-digitales-de-banco-central-189132> recuperado al 16/04/2020.

[271] Banco de Inglaterra, Discussion Paper, el *Futuro del Dinero*, Marzo de 2020, recuperado el 16/04/2020 en <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593>.

[272] Banco de Inglaterra, Discussion Paper, el *Futuro del Dinero*..o.c. p 5.

[273] Banco de Inglaterra, Discussion Paper, el *Futuro del Dinero*..o.c. p 6.

[274] Ibid.

[275] Confr. <https://www.coindesk.com/chinas-central-bank-testing-blockchain-backed-digital-currency>, recuperado el 16/04/2020.

[276] Confr. <https://es.cointelegraph.com/news/turning-a-crisis-into-an-opportunity-china-getting-one-step-closer-to-cbdc>, recuperado el 16/04/2020.

[277] Ibid.

[278] Confr. el muy interesante artículo escrito por Selva Ozelli, *Chinese blockchain-based mobile payment revolution: how the biggest CO2 polluter is becoming the World's leading producer of Solar Panels*, en <https://cointelegraph.com/news/chinese-blockchain-based-mobile-payment-revolution-how-is-the-biggest-co2-polluter-becoming-leading-world-solar-panels-producer> recuperado el 16/04/2020.

[279] Confr. Confr. Alexandra Sims, Kanchana Kariyawasam y David Mayes, *Regulating cryptocurrencies in New Zeland...o.c.*, p. 121.

[280] Ibid.

[281] Confr. Thibault Schrepel, *Libra: a concentrate of "Blockchain Antitrust"..o.c.*, cuya brillante investigación se seguirá como referencia para analizar el caso de Libra.

[282] Se recomienda la lectura del interesante análisis de Jameson Lopp, *Thoughts on Libra "Blockchain"*, disponible al 16/04/2020 en <https://blog.lopp.net/thoughts-on-libra--blockchain-/>, y Josh Constine, *Facebook announces Libra cryptocurrency: all you need to know*, disponible al 16/04/2020 en <https://techcrunch.com/2019/06/18/facebook-libra/>.

[283] Confr. <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>, disponible al 16/04/2020.

[284] Confr. <https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx>, disponible al 16/04/2020.

[285] Confr. Thibault Schrepel, *Libra: a concentrate of "Blockchain Antitrust"..o.c.*, p. 162. En nota 16, Schrepel indica que el PoS de Libra dispondría que los validadores tienen derechos de voto proporcionales a sus tenencias de Libra.

[286] Confr. Thibault Schrepel, *Libra: a concentrate of "Blockchain Antitrust"..o.c.*, p. 163.

[287] Confr. Jameson Lopp, *Thoughts on Libra “Blockchain”*, disponible al 16/04/2020 en <https://blog.lope.net/thoughts-on-libra--blockchain/>.

[288] Ibid.

[289] Ibid.

[290] Ibid.

[291] Confr. término empleado –con precisión– por Kevin Werbach, en *Trust, but verify...* o.c. p. 526.

[292] Confr. Nick Szabo, *The idea of Smart Contracts*, disponible en <https://perma.cc/YED2-ACVP>, conceptos que luego fueron ampliados en una publicación titulada *Formalizing and securing relationships on public networks*, disponible en: <https://perma.cc/U2L2-B34P>.

[293] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 505.

[294] Confr, Nick Szabo, https://en.wikipedia.org/wiki/Nick_Szabo.

[295] Confr. Nick Szabo, *The idea of Smart Contracts*, disponible en <https://perma.cc/YED2-ACVP>.

[296] Confr. Nick Szabo, *Formalizing and securing relationships on public networks*, disponible en: <https://perma.cc/U2L2-B34P>.

[297] Confr. Karen Yeung, en *Regulation by blockchain..* p. 223, nota 65.

[298] Confr. Nick Szabo, *Smart Contracts: building blocks for digital markets*, recuperado el 16/04/2020 en <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LC>

[299] El Código Civil y Comercial de la Nación en su Art. 957 define al contrato como “acto jurídico mediante el cual dos o más personas manifiestan su consentimiento para crear, regular, modificar, transferir o extinguir relaciones jurídicas patrimoniales.” El Art. 958, por su parte, consagra la libertad de contratar dentro de los límites legales; el Art. 959 declara su efecto vinculante; el Art. 960 dispone que los jueces no pueden modificarlos salvo si hay afectación del orden público; el Art. 961 consagra la buena fe en materia contractual y el Art. 962 dispone que en la materia contractual las normas son, por regla, supletorias de la voluntad de la partes. El Art. 965 por su parte declara que los derechos resultantes de los contratos integran el derecho de propiedad del contratante. El Art. 969 se refiere a las formas contractuales, y el Art. 970 recepta los contratos innominados.

[300] Eliza Mik, *Smart Contracts: terminology, technical limitations...o.c.*, p. 272.

[301] Eliza Mik, *Smart Contracts: terminology, technical limitations...o.c.*, p. 273.

[302] Eliza Mik, *Smart Contracts: terminology, technical limitations...o.c.*, p. 274.

[303] Confr. Riikka Koulu, en *Blockchains and Online Dispute Resolution: Smart Contracts as an alternative to enforcement*, publicado en ScriptEd, Vol. 13, Número 1, Mayo 2016, p. 57, sobre Solidity, aclara: “Solidity, the object-oriented programming language used within the Ethereum platform to draft smart contracts. **Object-oriented programming is based on “objects”, that are data structures containing both data fields (attributes) and procedures (methods).** The procedures of a software program can access and modify the data fields of other programs that they interact with. Objects are created based on templates called classes that define the initial values and methods or functions for the program. Fields are data organised within the classes or objects. Regular fields are also called instance variables, where there is a different variable for different instances (e.g. a class called “student” includes a field called “name” and each student has a distinct name). There are also static fields, where the field only has one variable that stays the same in all instances of the object (e.g. all students have the right to study). Smart contracts written with Solidity govern the behaviour of different accounts within Ethereum and the language is designed to correspond with such external concepts as ownership and identity. The basic structure of Solidity is the contract, which also forms a separate object on the blockchain. A contract deployed on the blockchain can be seen as an instance of a class.”El resultado es mío.

[304] Confr. David Black, *Blockchain smart contracts aren't Smart and aren't Contracts*, recuperado el 16/04/2020 en <https://www.forbes.com/sites/davidblack/2019/02/04/blockchain-smart-contracts-arent-smart-and-arent-contracts/#1e224ffb1e6a>.

[305] Karen Levy, *Book-smart, Not street-smart: blockchain-based smart contracts and the social workings of law*, disponible al 16/04/2020 en <https://estsjournal.org/article/view/107>, p. 3.

[306] Idem, p. 4.

[307] Idem, p. 10.

[308] Confr. Jonathan G. Rohr, *Smart contracts and traditional contract law, or: the law of the vending machine*, publicado en *Cleveland State Law Review*, Enero de 2019, Vol. 67, número 1, p. 68.

[309] Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 370.

- [310] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 527.
- [311] Confr. Karen Yeung, en *Regulation by blockchain..* p. 223.
- [312] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 505.
- [313] Confr. Max Raskin, en *The law and legality of smart contracts...* o.c. p. 3.
- [314] Confr. Tsui S. Ng, *Blockchain and beyond: Smart Contracts*, recuperado el 16/04/2020 en https://www.americanbar.org/groups/business_law/publications/blt/2017/09/09_ng/.
- [315] Vitalik Buterin, *A next-generation smart contract and decentralized application platform*, el White Paper de Ethereum, disponible en <https://github.com/ethereum/wiki/wiki/White-Paper> al 17/04/2020. En algún momento, Vitalik utilizó la expresión Smart Contracts con demasiado desapego a sus contornos legales, y reconoció luego públicamente que el término era erróneo y equívoco, por lo que generalmente estaba mal empleado, ya que no había un contrato legal subyacente en muchas ocasiones. Esto es cierto, y también lo inverso. Casos hubo –véase los T&Cs del TheDAO– en los que en la realidad on-chain existía un contrato legal subyacente, pero se intentó evitar las consecuencias de tal realidad, afirmando que la codificación en *machine-readable format* no generaría obligaciones en formato judicialmente ejecutable.
- [316] Confr. ETHEREUM, <https://www.ethereum.org>; Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, <http://gavwood.com/paper.pdf>, recuperado el 18/04/2020.
- [317] Confr. MultiChain: <https://www.multichain.com>.
- [318] Confr. Gideon Greenspan, *Why many smart contract use cases are simply impossible*, recuperado el 15/04/2020 en <https://www.coindesk.com/three-smart-contract-misconceptions>.
- [319] Confr. Aaron Wright y Primavera De Filippi, *Decentralized...* p. 10.
- [320] Idem, p. 11.
- [321] Confr. Aaron Wright y Primavera De Filippi, *Decentralized..* p. 10, nota 46.
- [322] Confr. Reggie O'Shields, *Smart Contracts: legal agreements for the blockchain*, publicado en 21 N.C. Banking Inst. 177 (2017), disponible al 18/04/2020 en: <http://scholarship.law.unc.edu/ncbi/vol21/iss1/11>, p. 179.

[323] Ibid.

[324] Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates: foundations, design landscape and research directions*, recuperado el 23/04/2020 en <https://arxiv.org/abs/1608.00771>, p. 2.

[325] Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction to smart contracts*, publicado en la revista polaca *Scientia Nobilitat*, en 2014, p. 4. Ejemplifican el funcionamiento de un contrato inteligente del siguiente modo: “*An appropriate analogy for the reader to envision would be that of two masters that share a servant; the latter has the ability to read and is bound to obey both his masters' signed instructions. When the two masters draft and sign an agreement; the servant, upon receipt of the written contract, would oversee and perform the contractual obligations through to the contract's termination. To draw the parallel back to SCs, the masters are the parties to the contract and the SC is the servant that executes the contract obligations.*”

[326] Confr. Riikka Koulu, en *Blockchains and Online Dispute Resolution: Smart Contracts as an alternative to enforcement*, publicado en ScriptEd, Vol. 13, Número 1, Mayo 2016, 53.

[327] Confr. Michèle Fink y Valentina Moscon, *Copyright law on blockchain: between new forms of rights administration and digital rights management 2.0*, publicado en *la International Review of Intellectual Property and Competition Law*, vol. 50, pag. 77–108, 2019, disponible al 15/04/2020 en <https://link.springer.com/article/10.1007%2Fs40319-018-00776-8>, p. 92.

[328] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 12.

[329] Confr. Chamber of Digital Commerce, *White Paper: Smart Contracts: is the Law ready?*, disponible al 16/04/2020 en <https://digitalchamber.org/smart-contracts-whitepaper/>, p. 10.

[330] The Cardozo Blockchain Project, “*Smart Contracts*” & *Legal Enforceability*, 2018, reporte n.º 2, recuperado el 16/04/2020 en <https://larc.cardozo.yu.edu/blockchain-project-reports/2>, p. 3.

[331] Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory framework of blockchains and smart contracts*, disponible al 16/04/2020 en <https://www.eublockchainforum.eu/reports>, p. 22.

[332] Ibid.

[333] Confr. Santiago Mora, *La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso*, publicado en La Ley 01/04/2019, cita online: AR/DOC/537/2019.

[334] Confr. Carlos Mirassou Canseco y Andrés Hadad, *Nuevo paradigma contractual: los smart contracts*, publicado en Sup. Esp. LegalTechII 2019 (noviembre), 11/01/2019, 49, cita online: AR/DOC/3578/2019.

[335] Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory framework of blockchains and smart contracts*, disponible al 16/04/2020 en <https://www.eublockchainforum.eu/reports>, p. 23.

[336] En la República Argentina, la regulación general de los contratos está contenida en el Código Civil y Comercial de la Nación, Libro III, *Derechos Personales*, Título II, *Contratos en general*, Capítulos I (Disposiciones generales), II (Clasificación de los contratos), III (Formación del Consentimiento), IV (Incapacidad e Inhabilidad para Contratar), V (Objeto), VI (Causa), y VII (Forma). Los Capítulos VIII, IX y X regulan la prueba, los efectos y la interpretación de los contratos, respectivamente. Si un contrato inteligente cumple los requisitos prescriptos en los Capítulos I-VII, entonces puede ser considerado un contrato para la legislación argentina.

[337] C.C.C.N., Art. 1015.

[338] C.C.C.N., Art. 984.

[339] C.C.C.N., Art. 985.

[340] C.C.C.N., Art. 988, inc. c.

[341] Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory...o.c.*, p. 25, se señala que se puede tratar de la representación *on-chain* –i.e., en blockchain– de bienes *off-chain* (inmuebles, etc.), o directamente de la representación digital de activos nativos *on-chain* (criptomonedas, o derechos de acceso, propiedad intelectual). La tokenización de activos off-chain se potencia sobremanera cuando se complementa con smart contracts. Ahora bien, cuando el activo es *per se* nativo digital, como una criptomoneda u otros tipos de tokens, sin ningún correlato subyacente y físico, aparecen allí los problemas de la naturaleza jurídica del token, situación que es aún más compleja cuando se crean tokens híbridos, sumado a todo ello la pseudonimia propia de los entornos blockchain.

[342] Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory...o.c.*, p. 27. Véase *supra* lo expuesto sobre DAOs y DACs en las notas 219 a

223. La naturaleza jurídica de una DAO y de sus miembros, es un punto en arduo debate en todo el mundo. Distintas legislaciones le asignan distinta naturaleza jurídica, incluyendo ser un contrato multilateral de organización no personificado, una sociedad simple, un contrato de colaboración, una sociedad con responsabilidad ilimitada, o una sociedad con responsabilidad limitada. La discusión abierta en este momento en todo el mundo, es si debiera reconocérseles a las DAOs personalidad jurídica diferenciada, o no, más allá de la dificultad práctica de determinar qué jurisdicción territorial es competente para asignarle un determinado status legal.

[343]

Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory...o.c.*, p. 31. Ciertos contratos inteligentes pueden programarse para tomar decisiones “por su cuenta”. ¿Puede un software ser considerado un representante de una parte? ¿Debiera desarrollarse una nueva categoría de persona, que no es humana ni jurídica, sino *electrónica*? Recordar siempre que el software, como cualquier creación humana, es falible y puede contener *bugs*. ¿Quién responde por los daños y perjuicios causados por un smart contract mal programado? ¿Hay un representado a quién demandar? ¿Debiera el representante contratar un seguro de responsabilidad civil por actuación digital perjudicial a terceros? Como señala el informe del Observatorio Europeo: “*The answers to such questions are important. There is always a possibility that a smart contract has a flaw, that the integrity of the blockchain is corrupted. In these situations questions of liability immediately arise, as has been set out above, putting coders, miners and other stakeholders at risk. To promote decentralised forms of cooperation on a DLT*

as means to develop commercial ventures, the cooperating entities - be they private or public

- may wish to run the blockchain/DLT and use applications on top through a legal vehicle. This can be a for-profit company (e.g.: LLP, GmbH, Société Anonyme) or a not-for-profit legal vehicle (e.g. foundation). Whatever the choice, implications for liability emerge. The choice of the legal vehicle and its registration also have immediate fiscal repercussions. It has so far not been explored whether legal vehicles available under national regimes suffice to serve as underpinning autonomous smart contracts and other forms of decentralised DLT co-operation that operate cross-border across regions and continents, or whether a specific new legal vehicle of a transnational nature would be required.” El resaltado es mío.

[344]

Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer’s introduction to smart contracts...o.c.*, p. 5, señalan que no es una novedad que ciertos términos contractuales sean parcialmente codificados para automatizar su ejecución, sin requerir actividades manuales. Por ejemplo, comprar una canción por iTunes: una vez confirmado el pago, el cumplimiento de la contraprestación se encuentra totalmente automatizado.

[345]

Ibid. Señalan Bourque y Tsui que en muchos casos el contrato convencional

subyacente es un contrato por adhesión, redactado por el vendedor, mientras que el código que ejecuta éstos términos no está incluido ni expuesto en ellos, está físicamente separado, en muchos casos siendo una práctica comercial poco transparente.

[346] Ibid. Es posible que el código esté bajo custodia del vendedor/proveedor, y que el comprador no tenga derecho a auditarlo, por razones de seguridad de los sistemas informáticos del vendedor. También es posible que el código del contrato esté bajo custodia y control de una tercera parte, con lo que ni el vendedor ni el comprador tienen control sobre el mismo, y en principio habría allí más transparencia sobre los términos codificados.

[347] Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates: foundations, design landscape and research directions*, recuperado el 23/04/2020 en <https://arxiv.org/abs/1608.00771>, p. 2, siguiendo a Josh Stark, *Making sense of blockchain smart contracts*, recuperado el 25/04/2020 en <https://www.coindesk.com/making-sense-smart-contracts>.

[348] Véase *infra* § 2.4.6.

[349] Véase *infra* § 2.5.3.

[350] Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction...o.c.* p. 17. Sostienen los autores que el smart contract sería el fiduciario, y las partes que lo programan serían fiduciantes y beneficiarios o fideicomisarios. El código programado es la manda fiduciaria, y el activo fiduciario serían los bienes que el smart contract controle. En nuestro derecho, el fiduciario debe ser una persona humana o jurídica.

[351] Ibid. Dado que un contrato inteligente puede ser programado para celebrar otros contratos, se ha considerado la posibilidad de considerarlo un representante convencional de la o las partes. Al igual que respecto del fiduciario, en nuestro derecho el representante debe ser una persona humana o jurídica.

Sin perjuicio de lo anterior, Riikka Koulu, o.c., p. 55, nota 50, señala que los consumidores –y los *prosumidores*, con más razón– podrían beneficiarse de smart contracts que los representen, existiendo un gran “*potential from the perspective of consumer protection in online transactions, where consumers' possibilities of negotiating their own contract terms has otherwise become compromised. He suggests that automated agents could help in restoring consumers' bargaining power by searching and concluding an online contract on their behalf without relying on e-commerce intermediaries' standard terms or revealing the consumers' identity beyond their capability to pay for the transaction. However, Fairfield identifies several challenges for actualising the potential of smart contracts: the technology is not yet commoditised, it is unclear, how companies will react to consumer- oriented contract terms and how*

individualised contract negotiations will affect overall transaction costs.” El resaltado es mío.

[352]

Ibid. ¿Podría un contrato inteligente ser considerado una persona jurídica? La discusión también se predica respecto de las DAOs y DACs, véase *supra* notas 219 a 223. El Art. 141 del CCCN reza: “*Son personas jurídicas todos los entes a los cuales el ordenamiento jurídico les confiere aptitud para adquirir derechos y contraer obligaciones para el cumplimiento de su objeto y los fines de su creación.*” El resaltado es mío.

[353]

Confr. Gabrielle Patrick y Anurag Bana, miembros del IBA Legal Policy & Research Unit Legal Paper, en *Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World*, recuperado el 10/05/2020 en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwi5zPvGwqnpAhUDHrkG520D-45FA-A29B-EF019A7D7FC9&usg=AOvVaw1Wtx9ZZkf0ltdfa1eqvS_f, p. 39.

[354]

Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer’s introduction to smart contracts...o.c.*, p. 23.

[355]

Confr. Harry Surden, *Computable Contracts*, publicado por la Universidad de California en Davis, en su Revista de Derecho, vol. 46, n° 629, disponible al 17/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216866.

[356]

Harry Surden, *Computable Contracts...o.c.*, p. 631, nota 1.

[357]

Puede ampliarse –en general– en la página de la INTERNATIONAL LEGAL TECHNOLOGY ASSOCIATION, <https://www.iltanet.org/about>, y en particular, sobre *Legal-AI* en: Joe Dysart, *AI removes the drudgery from legal due diligence*, recuperado el 14/04/2020 en <https://cacm.acm.org/news/233886-ai-removes-the-drudgery-from-legal-due-diligence/fulltext>, sosteniendo que “*AI due diligence software, found that AI was better at finding loopholes and other risks in proposed non-disclosure agreements than professional veterans*”; Ben Klaber, en *Artificial Intelligence and Transactional Law: Automated M&A Due Diligence*, recuperado el 14/04/2020 en <http://users.umiacs.umd.edu/~oard/desi5/additional/Klaber.pdf>, sosteniendo que los “*intelligent electronically stored information (ESI) management systems are now commonly used*” y afirmando que “*an integrated human and machine-learning process can identify, classify, organize, prioritize and highlight documents, which must be disclosed pursuant to some type of business combination agreement (e.g., stock purchase agreement), with higher efficacy and speed and lower cost than humans can alone*”. Para un mapeo de la variedad de servicios legales potenciados por la Inteligencia Artificial, véase, en general: Alex Crowley, *AI and legal services in 2020*, recuperado el 15/04/2020 en <https://www.iltanet.org/blogs/alex-crowley1/2020/02/04/ai-and-legal-services-in-2020?ssopc=1>.

[358]

Harry Surden, *Computable Contracts...o.c.*, p. 660, nota 120 y ss., trae como ejemplos “actuales” (en 2012) los contratos financieros de swap de tipos de cambio, y los contrato de opción sobre acciones, y contratos de distribución on line de contenidos digitales vía streaming que especifican jurisdicciones admitidas y no admitidas a través de datos vinculados al IP de una computadora.

[359]

Harry Surden, *Computable Contracts...o.c.*, p. 632.

[360]

El proceso por el cual los algoritmos permiten o facilitan que las computadoras entiendan el lenguaje natural (humano) se conoce como *Natural Language Processing* (NLP). Para una revisión del estado del arte a 2019 sobre el NLP aplicado al lenguaje contractual, véase Mark Sears, *AI challenges and why legal is a great place to kick-start great NLP*, recuperado al 16/04/2020 en <https://www.forbes.com/sites/marksears1/2019/05/14/ai-challenges-and-why-legal-is-a-great-place-to-kick-start-great-nlp/#56e5c87c4408>, quien sostiene que “*a machine can review in seconds what would take an expensive attorney hours to review. Heretik, a company based in Chicago, Ill., uses machine learning (ML), specifically NLP, to automate tasks related to the legal domain, such as contract review and project forecasting.*” El futuro llegó, hace rato.

[361]

Harry Surden, *Computable Contracts...o.c.*, p. 633.

[362]

Idem, p. 658. Se afirma allí que se pueden crear instrucciones computarizadas que reflejan la intención de las partes contratantes en ciertas cláusulas específicas, a través de datos que tienen un sentido específicamente asignado, y que permiten determinar si ciertos hechos *transformados en datos* son contestes con términos contractuales especificados *ex ante*. Y el resultado de tales instrucciones computables, servirá como un primer “chequeo” del cumplimiento del contrato, pudiendo o no convertirse en una consecuencia legal conclusiva.

[363]

Idem, p. 664. No todo término o condición contractual es *computable*. La semántica es la disciplina de las Ciencias de la Computación que estudia cómo traducir a lenguaje no humano las palabras o conceptos que tienen un sentido determinado en el lenguaje humano. Así, la claridad de Surden se trae, nuevamente, a colación: “*To tell a computer what a word means, in many cases, is to provide a translation between a given word and a set of computer instructions producing outputs that are consistent with what a person would understand the word to mean*” y “*it is sometimes possible to functionally convey meaning to computers, and that functional translation may be sufficient for particular computing purposes — including creating computable contract terms. In other words, given a particular concept, there may be a functional, computer-processable “translation” of the meaning of that word, if one can find a set of computer instructions, or data-relationships, that*

produce output that is consistent with what a person with a deep conceptual understanding would expect”. “The computer has been provided with a set of automatable computer instructions **resulting in outputs that are consistent with what a person, with a conceptual understanding of the term, would have intended** — an approximation of meaning based upon functional output.” Los resaltados son míos.

[364]

Idem, p. 636.

[365]

Idem, p. 667. La expresión *cláusulas legibles por una computadora*, en realidad significa que “parties wishing to create computable contract terms can sometimes (but not always) **devise a set of computer instructions that act as functional translations of contract terms. This permits automated comparisons, which can be consistent with the limitations that the parties intended to convey, but which employ computer processes to lower certain transaction costs. Computers can be told the meaning of the words directly, or they can be told how to find information necessary to determine what a word means**”. El resaltado es mío.

[366]

Idem, p. 642. Son ejemplo de un contrato electrónico los términos y condiciones de un WebSite, y la contratación vía e-mail, entre otros.

[367]

Idem, p. 650, sostiene que no todas las cláusulas deben ser “traducidas” a machine-readable format en un data-oriented contract, sino sólo aquéllas que (i) puedan ser convertidas a un lenguaje no humano, e.g., precios, fechas, cantidades, y (ii) tenga algún sentido de negocio (o económico) hacerlo.

[368]

Idem, p. 669. Surden introduce el concepto de *captured legal assertions*. “The general idea behind a “captured legal assertion” is to have a qualified person — **someone who has the ability to employ professional or subject matter judgment** — and have that person apply that judgment to a set of facts. We might sometimes “capture” the results of that judgment as computer- processable data ... parties can sometimes effectively **give the computer access to the results of an earlier judgment made by a person who does have the capacity to make such an assessment, by expressing those results as data.**”El resaltado es mío.

[369]

Confr. Harry Surden, *Computable Contracts...o.c.*, p. 651, los define como contratos convencionales, redactados en lenguaje humano, que se negocian y firman antes de comenzar a desarrollar los *data-oriented agreements*, y que establecen las condiciones de éstos últimos, cómo deben interpretarse específicamente los datos colectados, y cuáles serán las reglas para gestionar excepciones no anticipadas. Estos contratos, según Surden y en opinión que se comparte, son de gran importancia ya que vinculan (i) lo que las partes entendieron al momento de contratar –su intención expresada– y (ii) la representación computacional de sus obligaciones.

El Art. 1063 del CCCN, titulado *Significado de las palabras*, sostiene que “Las palabras

empleadas en el contrato deben entenderse en el sentido que les da el uso general, excepto que tengan un significado específico que surja de la ley, **del acuerdo de las partes o de los usos y prácticas del lugar de celebración** conforme con los criterios dispuestos para la integración del contrato. Se aplican iguales reglas a las **conductas, signos y expresiones no verbales** con los que el consentimiento se manifiesta”. El Art. 1065, titulado *Fuentes de interpretación*, sostiene que “Cuando el significado de las palabras interpretado contextualmente no es suficiente, se deben tomar en consideración: (a) las **circunstancias en que se celebró**, incluyendo las negociaciones preliminares; (b) la conducta de las partes, incluso la posterior a su celebración; y (c) la **naturaleza y finalidad del contrato**.”

Si la finalidad de las partes fuera la de celebrar un contrato computable, o un Smart Contract, sin dudas deberán celebrar un contrato convencional donde precisen el significado de las palabras y cómo éstas se reflejarán en el lenguaje de la máquina –que puede ser considerado un conjunto de **signos**–, precisando las circunstancias específicas que hacen conveniente y justifican que ciertas obligaciones se automaticen mediante un código de programación, cualquiera sea el lenguaje –**signos**– de programación empleado(s), e independientemente de su ejecución –i.e., transcripción en signos que la máquina entiende– en una cadena de bloques, o en servidores centrales controlados por cada parte contratante. [1] [SEP]

[370] Harry Surden, *Computable Contracts...o.c.*, p. 653, nota 93.

[371] Surden, o.c. p. 655 los define como contratos que fijan reglas de procedimiento sobre cómo incluir futuras cláusulas *data-oriented*, sin detenerse en el significado de éstas, sino enfocándose en la necesidad de dotar de carácter contractual a los datos que se ingresen, incluyendo reglas sobre cómo proceder si aparecen errores en los datos. En el caso de los contratos derivados, este *procedural agreement* es un “estándar” al que directamente las partes se remiten, como si fueran, *mutatis mutandis*, un INCOTERM. Confr. ISDA, *Legal guidelines for smart derivatives contracts: the ISDA Master Agreement*, Febrero de 2019, disponible el 16/04/2020 en <https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf>.

[372] Harry Surden, *Computable Contracts...o.c.*, p. 683.

[373] *Idem*, p. 689.

[374] *Idem*, p. 694. Surden se refiere a esta posibilidad como *autonomous computable contracting*, o bien podríamos decir *Smart Contracting* en terminología del año 2020. Constituye una práctica ya muy conocida en los mercados financieros, que entrenan y recurren a *trading algorithms*. Con razón indica Surden que para poder llegar al estadio de *autonomous computable contracting*, antes debe necesariamente transitarse

el camino de los *computable contracts*.

[375] Confr. Samuel Bourque, *Ethereum HK: Samuel Bourque on Smart Contracts and DAOs*, video de YouTube disponible el 24/04/2020 en <https://www.youtube.com/watch?v=cTYqRClh3Mo>.

[376] Confr. Samuel Bourque, *Ethereum HK: Samuel Bourque on Smart Contracts and DAOs*, video de YouTube disponible el 24/04/2020 en <https://www.youtube.com/watch?v=cTYqRClh3Mo>.

[377] Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 373. Véase también, del mismo autor, *Smart Contract Basics – A legal contract perspective*, recuperado el 16/04/2020 de <https://medium.com/fordham-business-law-association/smart-contract-basics-a-legal-contract-perspective-8da04b022973>.

[378] Ibid.

[379] Confr. Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels y Elaine Shi, *Town crier: an authenticated data feed for smart contracts*, disponible el 16/04/2020 en https://www.researchgate.net/publication/308691770_Town_Crier_An_Authenticated

[380] Confr. Gideon Greenspan, *Why many smart contract use cases are simply impossible.. o.c.*

[381] Confr. Eliza Mik, *Smart Contracts: terminology, technical limitations...o.c.*, p. 296.

[382] Las siguientes empresas ofrecen estos servicios: www.realitykeys.com y www.oracalize.it. Es también interesante el Oráculo de Thompson Reuters, *BlockOne IQ*. Véase <https://blockoneiq.thomsonreuters.com>

[383] Confr. Eliza Mik, *Smart Contracts: terminology, technical limitations...o.c.*, p. 298.

[384] Confr. Vitalik Buterin, *Ethereum and Oracles*, 22/07/2014, recuperado el 16/04/2020 en <https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/>.

[385] Confr. <https://www.swift.com/about-us>.

[386] Confr. <https://create.smartcontract.com/sibos17>, disponible al 15/04/2020.

[387] Confr. <https://www.financedigest.com/smartcontract-com-used-by-swift-announces-technical-leaders-as-advisors-launches-chainlink-to-connect-smart-contracts-to-off-chain-data-payments.html>, recuperado el 17/04/2020.

[388] Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 373.

[389] Confr. Jared Arcari, *Smart Contract Basics – A legal contract perspective Part II: Verifiability*, recuperado al 17/04/2020 en <https://medium.com/fordham-business-law-association/smart-contract-basics-a-legal-contract-perspective-part-ii-verifiability-4bc5c4ca8b88>.

[390] Ibid. Véase el caso de la empresa CodeLegit, confr. <https://datarella.com/codelegit-conducts-first-blockchain-based-smart-contract-arbitration-proceeding/>, recuperado el 18/04/2020.

[391] Ibid.

[392] Ibid.

[393] El CCCN consagra este principio en los Art. 1021 y 1022: “Regla general. El contrato sólo tiene efecto entre las partes contratantes; no lo tiene con respecto a terceros, excepto en los casos previstos por la ley.”

Art. 1022.- *Situación de los terceros. El contrato no hace surgir obligaciones a cargo de terceros, ni los terceros tienen derecho a invocarlo para hacer recaer sobre las partes obligaciones que éstas no han convenido, excepto disposición legal.*”

[394] Confr. Michael Smolenski, *Smart contracts: privacy vs. confidentiality*, recuperado el 16/04/2020 en <https://hackernoon.com/smart-contracts-privacy-vs-confidentiality-645b6e9c6e5a>.

[395] ZKP es un método de encriptación, un nuevo protocolo que permite agregar una nueva capa de seguridad para operar en blockchain. Permite que un usuario demuestre a otro que sabe o conoce un valor absoluto X, sin dar ninguna otra información sobre qué es o para que sirve X. Ampliar en Hasib Anwar, *What is ZKP? A complete guide to Zero Knowledge Proof*, recuperado el 16/04/2020 en <https://101blockchains.com/zero-knowledge-proof/#2>. Véase también el protocolo zk-SNARKs, acrónimo de *Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*, que refiere a una construcción de prueba en la que se puede **demostrar la posesión de cierta información**, por ejemplo, una clave secreta, **sin revelar esa información**, y sin ninguna interacción entre el proveedor y el verificador, disponible al 15/04/2020 en <https://z.cash/es/technology/zksnarks/>.

[396] Confr. Michael Smolenski, *Smart contracts...o.c.* afirma que los llamados *State Channels* permiten que en la blockchain solo se registre una referencia a una transacción exitosa, pero la transacción en sí no se realiza en la blockchain. Son muy útiles cuando hay micropagos entre dos partes, pero en alguna medida eliminan los atributos más sobresalientes de la blockchain: dejar un registro abierto, transparente e

inmutable.

[397]

Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 375.

[398]

La confidencialidad en materia contractual convencional está regulada en el Art. 992 del CCCN y en la Ley N° 24.766 (B.O. 30/12/1996). El primero dispone: “*Deber de confidencialidad. Si durante las negociaciones, una de las partes facilita a la otra una información con carácter confidencial, el que la recibió tiene el deber de no revelarla y de no usarla inapropiadamente en su propio interés. La parte que incumple este deber queda obligada a reparar el daño sufrido por la otra y, si ha obtenido una ventaja indebida de la información confidencial, queda obligada a indemnizar a la otra parte en la medida de su propio enriquecimiento.*”

La Ley 24.766, a su turno, dispone:

“Art.1°- *Las personas físicas o jurídicas podrán impedir que la **información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honesto, mientras dicha información reúna las siguientes condiciones:(a) sea secreta en el sentido de que no sea, como cuerpo o en la configuración, reunión precisa de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y (b) tenga un valor comercial por ser secreta; y (c) haya sido objeto de **medidas razonables, en las circunstancias, para mantenerla, secreta, tomadas por la persona que legítimamente la controla.*****

Se considerará que es contrario a los usos comerciales honestos el incumplimiento de contratos, el abuso de confianza, la instigación a la infracción y adquisición de información no divulgada por terceros que supieran o no, por negligencia grave, que la adquisición implicaba tales prácticas.

Art. 2°- *La presente ley se **aplicará a la información que conste en documentos, medios electrónicos** o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares.*”(el resaltado es mío).

[399]

La expresión *Altcoin* hace referencia a toda criptomoneda similar a bitcoin. A principios del año 2020, existen ya más de 5.000 altcoins, y representan el 34% de todo el cryptomarket. Confr. <https://www.investopedia.com/terms/a/altcoin.asp>, recuperado el 16/04/2020.

[400]

Confr. Michael Smolenski, *Smart contracts...o.c.* proponiendo un enfoque en este sentido a través de *LightStreams*, confr. <https://lightstreams.network>.

[401]

Confr. Jordan Clifford, *Privacy on the blockchain*, disponible al 18/04/2020 en <https://medium.com/hackernoon/privacy-on-the-blockchain-7549b50160ec>.

[402]

Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction to...* p.

13, indican que “Pseudo-anonymity is an interesting concept; it ought not to be as intimidating a term as it sounds. A simple way to look at it, is to examine how email addresses do not in-and-of themselves reveal the identity of the person; only if one has the email registered in his own address book would he know who the person is. There is no centralized registration of databases and new, free emails can be created on a whim. The same is true of cryptocurrency wallets. **The major difference is that wallets are not human-readable, to the point where one could perhaps not recognize his own wallet address.** Otherwise, all is unchanged, the cryptocurrency wallet address is a one-way unique identifier that guarantees reaching a person’s pocketbook, or inbox, but does not reveal the person’s identity (...) as **wallet addresses will not inherently provide any clues to the party’s identities.** An additional consideration is the encryption of the body of the SC. The authorities may attach the SC via injunction, but neither its content, nor the parties’ may be interpretable or identifiable without the parties’ encryption keys.” El resultado es mío.

[403]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 16.

[404]

Ibid.

[405]

Idem, p. 37, nota 82, se señala allí que “Like the government or any other authority, hackers are unable to interfere in blockchain because of public-key encryption”.. y que “When consumers send information over the internet, nearly anyone can get that information because it travels through many uncontrolled nodes. But, **public-key encryption guarantees that anyone reading the information cannot understand it unless they were accepted by the respective consumer to have the key.** If hackers could break public-key encryption they would instantaneously be able to influence and control a significant proportion of the existing wealth of nations.” El resultado es mío.

[406]

Idem, p. 18. ECDSA significa Elliptic Curve Digital Signature Algorithm. Señalan Kaal y Calcaterra que: “This scheme uses elliptic curve algebra in order to garble the message, but otherwise it is very similar to the RSA method of taking powers of large numbers with modular arithmetic. ECDSA also naturally incorporates a changing scale of encryption strength, which is one minor way bitcoin security responds automatically to improvements in computing power through the years, giving users long term confidence in the system. **The public-key algorithm makes the location and ownership of bitcoins as perfectly anonymous within the system as is practically possible.** Experts are confident this protocol will resist any foreseeable development in computing, such as changes in hardware like the imaginable switch from electronic to quantum computing.” El resultado es mío.

[407] Confr. Wulf A. Kaal y Craig Calcaterra..o.c., p. 23 sostienen: “*With the use of public-key cryptography and cryptographic hash functions, blockchain architecture gives its users long term confidence in anonymity, security, and decentralized autonomy. Users’ accounts are encoded by private keys, so their information is securely encrypted. They have complete power over whether they share information and with whom. When sharing generic information, such as the fact that they own more than 10 bitcoins, they reveal no private information. Further, each time a transaction is made, a new private key can be made. So, while we can track the public key of the addresses of each transaction, and that information is stored eternally in the blockchain, each transaction allows for an entirely new private identity which is cryptographically secured. This gives more anonymity in business transactions than ever before imagined.*” (el resaltado es mío).

[408] Idem, p. 48, nota 97, levantan el punto de la anonimidad versus la capacidad de almacenamiento de datos, en estos términos: “*The blockchain is immutable. All that is stored in blockchain remains there forever and cannot be deleted. This is a serious drawback, given that most of the information in the interaction of users can be temporary and it could be deleted when the need for its storage disappears. Eternal storage of information also works against anonymity. Each node is a complete replica of other nodes. As a result, with the explosive growth of the application's popularity on the blockchain, the size of the blockchain grows rapidly at all nodes simultaneously. At some point, the size of blockchain can exceed the capacity of mass-produced hard disks and for the operation of the nodes, special equipment will be required, which only large companies can afford, which leads to dangerous centralization.*” El resaltado es mío.

[409] Confr. <https://www.elliptic.co> y <https://www.chainalysis.com>, citados por Jordan Clifford, *Privacy on the blockchain...o.c.*

[410] Confr. <https://bitcointalk.org/index.php?topic=279249.0> y <https://themerke.com/top-4-reliable-bitcoin-mixers/>, citados por Jordan Clifford, *Privacy on the blockchain...o.c.*

[411] Confr. Konstantinos Christidis y Michael Devetsikiotis, en *Blockchains and Smart Contracts for the Internet of Things....o.c.*, p. 2300.

[412] Confr. Pedro Febrero, *What on-chain analytics tell us about bitcoin transactions in 2020?* Recuperado el 16/04/2020 en <https://cointelegraph.com/news/what-on-chain-analytics-tell-us-about-bitcoin-transactions-in-2020>.

[413] UTXO significa Unspent Transaction Output. Ampliar en Steven Buchko, *What is a UTXO? A beginner’s explainer on transactions outputs*, disponible al 16/04/2020 en

<https://coincentral.com/utxo-beginners-explainer/>.

[414]

Confr. Jordan Clifford, *Privacy on the ...o.c.*

[415]

Confr. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen y Charalampos Papamanthou, *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*, recuperado el 16/04/2020 en <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7546538>.

[416]

Ampliar en Ameer Rosic, *Cryptocurrency Wallet Guide: a step-by-step tutorial*, disponible al 16/04/2020 en <https://blockgeeks.com/guides/cryptocurrency-wallet-guide/>.

[417]

Ibid.

[418]

La tragicomedia ocurrió en 2013, cuando sin querer una persona tiró un pen drive, que contenía la llave privada asociada a una llave pública que tenía 7.500 bitcoins. Ampliar en <https://cointelegraph.com/news/infamous-discarded-hard-drive-holding-7500-bitcoins-would-be-worth-80-million-today>, recuperado al 16/04/2020.

[419]

Aunque se está avanzando en técnicas de recuperación de llaves privadas. Ampliar en Antoine Herzog, *Private key recovery – decentralize user's responsibility*, disponible al 15/04/2020 en <https://medium.com/iov-internet-of-values/private-key-recovery-decentralize-users-responsibility-88fa60ee905>.

[420]

Confr. Connor Blenkinsop, *How to recover your wallet if your private keys are lost*, recuperado el 16/04/2020 en <https://cointelegraph.com/news/how-to-recover-your-wallet-if-your-private-keys-are-lost>.

[421]

Sirve de muestra el ejemplo del robo ocurrido en Enero de 2018 en Japón por un monto cercano a los 500 millones de Dólares en una criptomoneda llamada NEM. La víctima fue un *Exchange* japonés llamado CoinCheck, que alojaba todas las llaves privadas de las cuentas de sus clientes en una *hot wallet*. Es el segundo robo más grande en la historia de las criptomonedas, luego del caso Mt Gox en 2014, de donde se robaron una cantidad de bitcoins que en aquel momento equivalía al 6% de todo el circulante, llevando a la quiebra a Mt Gox.

En el caso CoinCheck traído a colación, se robaron 500 millones de tokens de la criptomoneda NEM, que se distribuyeron luego en 19 direcciones de la blockchain. CoinCheck indemnizó a los 260.000 usuarios perjudicados y desde la Fundación NEM se identificó los 500 millones de tokens robados, colocando un aviso para que todo el mundo supiera que eran robados y se identificó e hizo públicas once direcciones que alojaban parte de los tokens robados, pero sin saberse quiénes eran los dueños de las cuentas. Los ladrones finalmente pudieron cambiar los tokens en

exchanges no regulados, que no tienen procedimientos de KYC y AML. Ampliar en Brian Curran, *The history of the CoinCheck Hack: one of the largest Heists ever*, disponible al 16/04/2020 en <https://blockonomi.com/coincheck-hack/>.

[422]

Confr. Will Douglas Heaven, *Sitting with the cyber-sleuths who track cryptocurrency criminals*, MIT Technology Review, 19 de Abril de 2018, recuperado el 16/04/2020 en <https://www.technologyreview.com/2018/04/19/3011/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals/>.

[423]

Ibid.

[424]

Ibid.

[425]

Para ampliar sobre desarrollos actuales del clustering, véase la obra de Sudarshan S. Chawathe, *Clustering blockchain data: techniques, toolboxes and applications*, publicado en el libro *Clustering Methods for Big Data Analytics*, y disponible al 15/04/2020 en https://www.researchgate.net/publication/328570658_Clustering_Blockchain_Data_Techniques_Toolboxes_and_Applications.

[426]

Confr. Will Douglas Heaven, *Sitting with the cyber-sleuths...o.c.*

[427]

Véase <https://z.cash/es/>.

[428]

Véase <https://www.getmonero.org>.

[429]

Ampliar en <https://cointelegraph.com/news/us-prosecutors-indict-btc-e-crypto-exchange-seek-millions-in-penalties>, recuperado el 16/04/2020.

[430]

Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 375.

[431]

Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates...o.c.* precisan que “We say that a smart contract is “**automatable**” rather than that it is “automated” because in practice **there may be parts of a legal agreement whose performance requires human input and control**. However, to be a “smart contract” we require that some part of the agreement is capable of being automated (otherwise it is not “smart”). **Automation is generally accomplished by the use of one or more computers. The phrase “by electronic means” is a synonym**. Our definition of smart contract does not require that this automation occurs on a shared ledger, though that is certainly a possible and even probable method.” El resaltado es mío.

[432]

El CCCN dispone en su Art. 390: “Restitución. La nulidad pronunciada por los jueces **vuelve las cosas al mismo estado en que se hallaban antes del acto declarado nulo** y obliga a las partes a restituirse mutuamente lo que han recibido. Estas restituciones se rigen por las disposiciones relativas a la buena o mala fe según sea el

caso, de acuerdo a lo dispuesto en las normas del Capítulo 3 del Título II del Libro Cuarto.”

[433]

Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates...* o.c. p. 3 ejemplifican tales causas extrañas al contrato inteligente con deficiencias en la entrega física de bienes.

[434]

Idem, p. 4, ven con cierto temor la posibilidad real de implementar medios no tradicionales de resolución de conflictos para contratos inteligentes, ya que: (i) los sistemas distribuidos como la blockchain, no permiten modificar el código de un smart contract una vez iniciado; (ii) los contratos de la vida real normalmente necesitan un “ajuste dinámico”, y todos estos ajustes debieran forzosamente ser codificados *ex ante* si el contrato corre en una blockchain; (iii) el cumplimiento forzoso dentro de la red sólo puede referirse a derechos y obligaciones que están “dentro de la red”, quedando afuera objetos y derechos off-chain; y (iv) para el caso de smart contracts que permiten automatizar pagos, para prevenir posibles perjuicios por ejecución deficiente, debieran constituirse garantías que también operarían de modo automático, quedando afectadas siempre al contrato que “afianzan”. Estas garantías pueden afectar la liquidez del mercado, y su capacidad de apalancamiento financiero.

[435]

Ibid.

[436]

En el caso de EE.UU, legislación a nivel federal (Uniform Commercial Code y la *Electronic Signatures in Global and National Commerce Act*, conocida como la *E-Sign Act*) así como legislación estadual que sigue el modelo de la *Uniform Electronic Transactions Act* los ha reconocido como contratos sin mayores reparos.

[437]

El CCCN dispone en su Art. 1084: “*Configuración del incumplimiento. A los fines de la resolución, el incumplimiento debe ser esencial en atención a la finalidad del contrato. Se considera que es esencial cuando: (a) el cumplimiento estricto de la prestación es fundamental dentro del contexto del contrato; (b) el cumplimiento tempestivo de la prestación es condición del mantenimiento del interés del acreedor; (c) el incumplimiento priva a la parte perjudicada de lo que sustancialmente tiene derecho a esperar; (d) el incumplimiento es intencional; (f) el incumplimiento ha sido anunciado por una manifestación seria y definitiva del deudor al acreedor.*” [SEP]

[438]

El CCCN dispone en su Art. 1104: “*Contratos celebrados fuera de los establecimientos comerciales. Está comprendido en la categoría de contrato celebrado fuera de los establecimientos comerciales del proveedor el que resulta de una oferta o propuesta sobre un bien o servicio concluido en el domicilio o lugar de trabajo del consumidor, en la vía pública, o **por medio de correspondencia**, los que resultan de una convocatoria al consumidor o usuario al establecimiento del proveedor o a otro sitio, cuando el objetivo de dicha convocatoria sea total o parcialmente distinto al de la*

contratación, o se trate de un premio u obsequio.” El resaltado es mío.

[439]

El CCCN dispone en su Art. 1105: “*Contratos celebrados a distancia. Contratos celebrados a distancia son aquellos concluidos entre un proveedor y un consumidor con el uso exclusivo de medios de comunicación a distancia, entendiéndose por tales los que pueden ser utilizados sin la presencia física simultánea de las partes contratantes. En especial, se consideran los medios postales, electrónicos, telecomunicaciones, así como servicios de radio, televisión o prensa.*” El resaltado es mío.

El Art. 1110, por su parte, dispone: “*Revocación. En los contratos celebrados fuera de los establecimientos comerciales y a distancia, el consumidor tiene el derecho irrenunciable de revocar la aceptación dentro de los diez días computados a partir de la celebración del contrato.*

Si la aceptación es posterior a la entrega del bien, el plazo debe comenzar a correr desde que esta última se produce. Si el plazo vence en día inhábil, se prorroga hasta el primer día hábil siguiente.

Las cláusulas, pactos o cualquier modalidad aceptada por el consumidor durante este período que tengan por resultado la imposibilidad de ejercer el derecho de revocación se tienen por no escritos.”

Por su parte, se consagran algunas excepciones a la facultad de revocación en el Art. 1116: “**Excepciones al derecho de revocar.** Excepto pacto en contrario, el derecho de revocar no es aplicable a los siguientes contratos: (a) los referidos a productos confeccionados conforme a las especificaciones suministradas por el consumidor o claramente personalizados o que, por su naturaleza, no pueden ser devueltos o puedan deteriorarse con rapidez; (b) los de suministro de grabaciones sonoras o de video, de discos y de programas informáticos que han sido decodificados por el consumidor, así como de ficheros informáticos, suministrados por vía electrónica, susceptibles de ser descargados o reproducidos con carácter inmediato para su uso permanente; y (c) los de suministro de prensa diaria, publicaciones periódicas y revistas.” Los resaltados son míos. ^[L]_[SEP]

[440]

El CCCN dispone en su Art. 1106: “*Utilización de medios electrónicos. Siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un soporte electrónico u otra tecnología similar.*” El resaltado es mío.

[441]

El CCCN dispone en su Art. 1107: “*Información sobre los medios electrónicos. Si las partes se valen de técnicas de comunicación electrónica o similares para la celebración de un contrato de consumo a distancia, el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos*” El resaltado es mío.

[442] Confr. The Cardozo Blockchain Project, “Smart Contracts” & *Legal Enforceability*,...o.c., p. 5.

[443] Confr. The Cardozo Blockchain Project, “Smart Contracts”..o.c., p. 6.

[444] Confr. UJO Music, <https://ujomusic.com>. Ampliar en <https://www.forbes.com/sites/jonathanchester/2016/09/16/how-blockchain-startups-are-disrupting-the-15-billion-music-industry/#2b947e6a407c>, recuperado el 16/04/2020 y en <https://medium.com/humanizing-the-singularity/smart-contracts-for-the-music-industry-3e641f87cc7>, recuperado el 16/04/2020.

El smart contract de UJO Music permite que cuando alguien escucha una canción bajada desde UJO Music, la plataforma “...*automatically triggers an agreement for everyone involved in the creative process of a song with those who choose to interact with it — fans, streaming services, or film crews (...)* It was the first song to automatically **distribute payments via a smart contract to all creatives involved in the making and recording of the song.**”

[445] Confr. OpenBazaar, <https://openbazaar.org>. Ampliar en <https://openbazaar.org/blog/Escrow-Smart-Contract-Specification-in-OpenBazaar/>, recuperado el 17/04/2020.

El smart contract de OpenBazaar es un *escrow agreement*, un depósito en garantía. Aquí se describe su funcionamiento: “*When a buyer and seller have agreed on a product and a price, the buyer sends their funds to an escrow address, which is a 2-of-3 multisig address with one key controlled by the buyer, one key controlled by the seller, and one key controlled by a moderator that has been agreed upon by both the buyer and the seller. On the “happy path”, the seller delivers the goods, then the buyer releases the funds to the seller (with the buyer and seller signing the payout transaction from the escrow address).*

In the event that the seller does not deliver the goods as promised, the buyer pleads their case to the moderator, and the buyer & moderator can send the funds from escrow back to the buyer.

In the (very common) case where the buyer receives their goods but doesn’t release the funds to the seller, the seller presents their case to the moderator, and the seller & moderator sign the funds from escrow to the seller. The seller can also unilaterally release funds from escrow after a previously agreed upon amount of time has passed. This allows the seller to release the funds from escrow without the moderator in the event that the buyer disappears. With UTXO-based coins, this is achieved by requiring that the buyer sign an nLockTime transaction releasing funds to the seller, and then passing that transaction to the seller (off-chain) before the seller delivers the product or service.”

[446] Visitar <https://safemarket.github.io>, con una propuesta de valor similar a OpenBazaar.

[447] Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates..o.c.*, p. 5 denominan “*aspectos operacionales*” a aquellas cláusulas de un contrato convencional que serían automatizadas. Respecto de tales aspectos y cláusulas, señalan los autores que es posible y conveniente estudiar las “equivalencias semánticas” entre el lenguaje natural legal, y el lenguaje de programación que codifica una cláusula.

[448] Ibid. A estas cláusulas las denominan “*aspectos no operacionales*”: son los que no se pueden o no conviene que se automaticen.

Con muchísima claridad, Clack, Bakshi y Braine señalan que “***The operational aspects of a contract would typically dictate the successful performance of the contract to completion. If a dispute arises, then the non-operational aspects of the contract would typically dictate what happens next — i.e. in the context of the rights and obligations of the parties, the specification of what remedies shall be applied in the case of contract partial-performance or non-performance by one party. The greater part of a legal contract may often be devoted to defining the rights and obligations of the parties in the event of a problem. Sometimes, the actions to be taken in case of material breach of contract are expressed precisely; however, this is not always the case and dispute resolution may require a protracted process of negotiated settlement, arbitration, or court proceedings. Furthermore, it is important to understand the role of law. A lawyer would read and understand the contract in the context of the governing law — i.e. each legal document must be interpreted according to the relevant law (corporate law, consumer law, etc.) of its stated or inferred jurisdiction, and therefore the semantics of that law must also be understood. It should be noted that the issue of law relates not only to the non-operational aspects but also to the operational aspects —for example, trading with certain countries may be illegal due to government-imposed sanctions.***”

[449] Confr. The Cardozo Blockchain Project, “*Smart Contracts*”..o.c., p. 6.

[450] Ibid.

[451] Id., p. 7. Se afirma que gracias a los Oráculos, los smart contracts se pueden adaptar a nuevas condiciones prácticamente en tiempo real. Incluso, se pueden delegar en Oráculos humanos i.e., abogados, la constatación del cumplimiento de ciertas obligaciones que no pueden ser fácilmente codificadas.

[452] Ibid.

[453] Para ampliarse sobre el *software testing*, véase:

<https://www.guru99.com/software-testing-introduction-importance.html>, recuperado el 16/04/2020; en <https://medium.com/better-programming/how-to-test-ethereum-smart-contracts-35abc8fa199d>, recuperado el 18/04/2020; y en [https://dev.to/smarty/how-to-test-ethereum-smart-contracts-audit-best-practices-53kg](https://dev.to/smarty/https://dev.to/smarty/how-to-test-ethereum-smart-contracts-audit-best-practices-53kg), recuperado el 17/04/2020.

[454] Confr. Reggie O'Shields, *Smart Contracts: legal agreements...* o.c. p. 193.

[455] Se sigue, en general, la exposición de Eliza Mik, *Smart Contracts: terminology, technical limitations...* o.c., p. 298.

[456] Confr. Eliza Mik, *Smart Contracts: terminology, technical limitations...* o.c., p. 277.

[457] Idem, p. 280.

[458] Idem, p. 281.

[459] Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction...* o.c. p. 17.

[460] Ibid.

[461] Pueden consultarse los siguientes casos ya detectados: eventos vinculados al software *Parity*: <https://www.coindesk.com/ethereum-client-bug-freezes-user-funds-fallout-remains-uncertain>, recuperado el 20/04/2020; en relación a un ataque reciente realizado el 31/12/2019, véase: <https://www.crowdfundinsider.com/2020/01/155850-hackers-exploited-parity-node-bug-to-attack-ethereum-network-december-30th/>, recuperado el 20/04/2020.

Sobre errores de codificación en el HKG token, véase: <https://bitcointalk.org/index.php?topic=1744115.0>, recuperado el 20/04/2020.

Sobre errores de codificación en el compilador de Ethereum, Viper, que es el encargado de traducir de lenguaje de programación al lenguaje que puede ser procesado por la EVM, véase: <https://es.cointelegraph.com/news/bugs-found-in-compiler-for-readable-ethereum-smart-contracts-team-downplays-concerns>, recuperado el 20/04/2020. Otros bugs en Ethereum son señalados por Stegeman, o.c. en nota siguiente.

Sobre posibles soluciones a las vulnerabilidades de programación de smart contracts, se recomienda la lectura del interesantísimo artículo de Shuai Wang, Chengyu Zhang y Zedong Su, *Detecting nondeterministic payment bugs in Ethereum smart contracts*, disponible al 20/04/2020 en <http://chengyuzhang.com/paper/oops19.pdf>.

[462] Confr. Lars Stegeman, *Solitor: runtime verification of Smart Contracts*, recuperada al 21/04/2020 en https://fmt.ewi.utwente.nl/media/LarsStegeman_SmartContractRuntimeVerifica p.4. La tesis de maestría de Stegeman propone una herramienta para Solidity que permite detectar *bugs*, a la que nomina *Solitor*. Excede ampliamente el objeto de este Manual, y principalmente la capacidad de su autor, emitir un juicio sobre la utilidad, conveniencia o aplicabilidad real de *Solitor*.

[463] Véase la interesante herramienta propuesta por Yi Zhou, Deepak Kumar, Surya Bakshi, Joshua Mason, Andrew Miller y Michael Bailey, *Erays: reverse engineering Ethereum's opaque smart contracts*, recuperado el 21/04/2020 en <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-zhou.pdf>.

[464] Idem, p. 288.

[465] Idem, p. 289.

[466] Confr., CCCN Art. 1061 y siguientes.

[467] El CCCN, en su Art. 1065 dispone: “*Fuentes de interpretación. Cuando el significado de las palabras interpretado contextualmente no es suficiente, se deben tomar en consideración: (a) las circunstancias en que se celebró, incluyendo las negociaciones preliminares; (b) la conducta de las partes, incluso la posterior a su celebración; y (c) la naturaleza y finalidad del contrato.*” El resaltado es mío. ^[1]_{SEP}

[468] Confr. Riikka Koulu, *Blockchains and Online Dispute Resolution...o.c.* p. 65.

[469] Confr. Eliza Mik, *Smart Contracts: terminology, technical...o.c.*, p. 291.

[470] Ibid.

[471] Idem, p. 293.

[472] Ibid.

[473] Idem, p. 294.

[474] Confr. Ari Juels, Ahmed Kosba y Elaine Shi, *The ring of Gyges: investigating the future of Criminal Smart Contracts*, recuperado el 17/04/2020 en https://www.researchgate.net/publication/310821111_The_Ring_of_Gyges_Investigati

[475] El ransomware es un tipo de delito cibernético que consiste en encriptar la

información dentro de una computadora, y exigir el pago de un “rescate” para descifrarla. Ampliar en <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html> disponible al 15/04/2020.

[476]

El célebre caso *Silkroad* sustenta muy bien el punto. Ampliar en <https://medium.com/@gritarespoco/silk-road-y-el-cibermercado-ilegal-c45967853f46>, recuperado el 18/04/2020. Véase también *infra* en 3.2.1.1.

[477]

Ampliar en <https://www.wired.com/2014/04/dark-wallet/>, recuperado el 18/04/2020. Durante el año 2019, aproximadamente 4.500 millones de Dólares se perdieron por esquemas fraudulentos en Bitcoin, robos de criptomonedas, y ciberataques a *Exchanges*, confr. CipherTrace, *Q4 2019 cryptocurrency anti-money laundering report*, disponible al 19/04/2020 en <https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/>. En 2018, este tipo de actividad ilegal representó pérdidas por 1.360 millones de Dólares, confr. Vandana Beessoo, *Money laundering through Bitcoin: the emerging implications of technological advancement*, disponible el 19/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3468300&download=yes.

[478]

Confr. Ari Juels, Ahmed Kosba y Elaine Shi, *The ring of Gyges...* o.c. p. 2.

[479]

Ampliar en <https://github.com/darkwallet/darkleaks>, recuperado el 18/04/2020.

[480]

Confr. Ari Juels, Ahmed Kosba y Elaine Shi, *The ring of Gyges...* o.c. p. 6.

[481]

Idem, p. 10.

[482]

Confr. Hisashi Oki, *Blacklists aren't enough to stop crypto fraud*, recuperado el 18/04/2020 en <https://cointelegraph.com/news/blacklists-arent-enough-to-stop-crypto-fraud>.

[483]

Confr. Max Boddy, *US Treasury targets crypto addresses of alleged narcotics traffickers*, recuperado el 18/04/2020 en <https://cointelegraph.com/news/us-treasury-sanctions-bitcoin-litecoin-addresses-under-kingpin-act>.

[484]

Confr. Ari Juels, Ahmed Kosba y Elaine Shi, *The ring of Gyges...* o.c. p. 13.

[485]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction ...* o.c. p. 40 aclaran el punto en estos términos: “*an Ethereum transaction is a complete smart contract. Therefore, the whole contract is either added to the blockchain or not. An Ethereum transaction can't be partially added to the blockchain. The second interpretation is the contract transactions between the parties. It is possible that parties can partially fulfil a smartcontract. But in that case the smart contract already has all eventualities accounted for—it is completely self-executing and self-regulating. Therefore, if one*

provision of the contract is fulfilled and another is not, the consequences of that situation is already stipulated in the code with mathematical inevitability. Whatever the program stipulates will happen, happens; including if nothing happens.” El resaltado es mío.

[486]

Confr. Konstantinos Christidis y Michael Devetsikiotis, en *Blockchains and Smart Contracts for the Internet of Things...*o.c., p. 2300, quienes ejemplifican la integración dual del siguiente modo: “(a) *deploy the smart contract in question, record its address on the blockchain, and **include that address in the real contract*** (b) *hash the corresponding real-world contract, record its hash digest, store the real contract in a safe space (can be centralized, or decentralized), (c) **send a transaction to the smart contract that includes the real contract’s hash in its metadata; the contract then stores that piece of information in its own, internal database. In case of a legal dispute, you can point to the hash stored in the smart contract, then present the real-world contract (that is uniquely identified by that hash) and **prove the link between the actions on the blockchain and the expected outcome in the physical world.*****” El resaltado es mío.

[487]

Ampliar en <https://www.w3.org/2016/04/blockchain-workshop/interest/hazard-hardjono.html>, recuperado el 22/04/2020.

[488]

Confr. <https://medium.com/@OpenLawOfficial/accelerating-the-transformation-of-the-legal-industry-9d349535190f> recuperado el 22/04/2020.

[489]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction ...*o.c. p. 38.

[490]

Ibid.

[491]

Ibid, véase también nota 83 y doctrina allí citada.

[492]

Idem, p. 41. Ampliar sobre contratos inteligentes reversos *infra* en § 2.6.

[493]

Confr. Reggie O’Shields, *Smart Contracts: legal agreements for ...*o.c. p. 191 indica que el operador de una blockchain puede estipular qué ley será aplicable y quién será el juez competente para los contratos que en ella se ejecuten.

[494]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction ...*o.c. véase en particular notas 84 y 85 y doctrina allí citada.

[495]

Idem, p. 43. Sostienen los autores citados que: “*The exercise of traditional jurisdictional means over the creator of blockchains may encounter problems over time. First, it is only a matter of time until blockchains are created by other blockchains. Moreover, governing the creation of blockchains may encounter practical **problems associated with anonymity. For instance, Satoshi, the billionaire founder of bitcoin is unknown and most hackers make it their personal hobby to ascertain his/her identity.***”

[496] Idem, p. 39 y nota al pie 88.

[497] Confr. Reggie O'Shields, *Smart Contracts: legal agreements...* o.c. p. 190.

[498] Confr. Riikka Koulu, en *Blockchains and Online Dispute Resolution: Smart Contracts as an alternative to enforcement*, publicado en ScriptEd, Vol. 13, Número 1, Mayo 2016, 42.

Señala Koulu “Despite, or more likely due to its origins in the 1990s, ODR still lacks a uniform definition. Some use the term to refer only to **privately organised models of technology- augmented dispute resolution, while others include courtroom technology, e.g. e-filing and case management systems, videoconferencing and automated document generation**. In short, ODR tools, models and applications vary significantly, but they all have in common the implementation of technology to dispute resolution in order to provide more efficient conflict management. ODR applications may exist separately, linked with public courts or as an integral part of e-commerce sites, as is the case with eBay’s Resolution Center. **Due to the constraints of territorial jurisdiction, state sovereignty and the newness of ODR, there are no global legal instruments for regulating legal issues related to cross- border ODR**. This means that the choice of law or jurisdiction, or the recognition and enforcement of ODR decisions, are all determined based on national law, which may often lead to complications in cross-border situations. In response to these challenges, the EU has created a union-wide ODR platform with translation services through the ODR Regulation (524/2013) and ADR Directive (2013/11/EU). Also, the United Nations Commission on International Trade Law (UNCITRAL) has attempted to draft uniform procedural rules for ODR but the work has come to a relative standstill.” El resaltado es mío. Para un análisis del estado actual de la cuestión de los ODRs y cloud computing contracts, véase UNCITRAL, *Draft notes on the main issues of Cloud Computing Contracts*, en <https://uncitral.un.org/en/cloud/dispute%20resolution>, disponible al 20/04/2020. Para una revisión de los ODRs y derecho del consumidor, véase Mirèze Philippe, *ODR redress system for consumer disputes*, recuperado el 20/04/2020 en https://www.elevenjournals.com/tijdschrift/ijodr/2014/1/IJODR_2014_001_001_004.p Para un análisis del funcionamiento de la ADR Directive, véase: https://ec.europa.eu/info/alternative-dispute-resolution-reports_en, recuperado el 20/04/2020.

[499] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 4. En efecto, en la página 46 afirman los citados autores que “as **Ethereum and other blockchain-based smart contracting networks become increasingly autonomous, legislators simply will not have the ability and authority to dictate to contracting parties and Ethereum itself whether or not to code existing legal rules into a given smart contract. Anonymity means the**

government cannot identify citizens with access to a free internet who use the blockchain. Nor can the government prevent citizens from adding contracts anonymously to the blockchain. Autonomy means the government cannot stop the blockchain miners from automatically adding contracts because the protocols do not recognize distinctions between good and bad contracts that any outside body dictates (as miners are also anonymous.) Also, the distributed nature of the blockchain means the government cannot control the nodes which maintain the blockchain without an effective world-wide governing body—which is obviously nowhere near feasible at this point in history—not even if the nodes were known to the government, which they are not.” Los resaltados son míos.

[500]

Confr. Riikka Koulu, en *Blockchains and Online..o.c.*, p. 55, quien también afirma, en opinión que se comparte, que “**Self-executing contracts might significantly alter dispute resolution, although it is unlikely that disputes will disappear completely.** *It is more likely that disputes themselves will change in step with the change of the methods for resolving them. Therefore, the challenge created by smart contracts is not directed simply to contractual law but is also relevant to dispute resolution and due process.*” El resaltado es mío.

[501]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute ..o.c.* p. 7.

[502]

Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer’s introduction...* p. 13, indican que “*the Smart Contract is not physically located, nor administered in any one specific physical location. In actuality, it is copied worldwide in a consensus network that guarantees its integrity. In a sense, it is both everywhere and nowhere. Such Smart Contracts without seat are technically possible with current technology on Ethereum.*”

[503]

Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute ..o.c.* p. 36. Señalan, con relación a la competencia territorial de los Tribunales, que “*..the concept of location or presence in jurisdictional means does not apply to the blockchain. A location for the blockchain does not exist - not physically or even electronically. Nodes that contain the blockchain and all of its information are located all over the world. Transactions in the blockchain are fully networked and “present” only in cyberspace. The nodes hold imperfect partial copies of the blockchain; no particular node holds the entire blockchain.*” El resaltado es mío.

[504]

Idem, p. 45, indicando que la “supra-nacionalidad” en este contexto se vincula, como contracara, con la (deseada) extraterritorialidad de ciertas leyes y regulaciones nacionales, y, a su turno, con la dificultad real de poder hacer cumplir tales efectos “extra-nacionales” fuera de las fronteras de un país, y especialmente dentro del entorno blockchain.

[505]

Idem, p. 7. Sostienen allí que la “*anonymity gained by the use of public-key*

encrypted identities and VPNs prevents the identification of the parties to a smart contract. Without identifiable parties, jurisdictional principles such as subject matter jurisdiction, personal jurisdiction, diversity jurisdiction, and federal question jurisdiction become irrelevant.” El resaltado es mío.

[506]

Idem, p. 28.

[507]

Idem, p. 35. Sostienen los autores citados, en opinión que se comparte, que los *blockchain-based smart contracts* crearán un nuevo y especial entorno contractual digital, hasta ahora desconocido, y muy distinto a la contratación vía Internet que se ha desarrollado desde 1995 a 2020.

Así, en una transacción usual de Internet: (i) las partes que contratan son conocidas, sea de modo directo o de modo indirecto a través de los Internet Service Providers, (ii) si las partes no son conocidas, la dirección de IP de una persona sí es conocida, (iii) se pueden conocer los detalles de la propiedad objeto de la transacción, y también la mecánica de pagos empleada, (iv) los pagos se hacen en moneda convencional, no en criptomonedas, (v) y todo lo anterior ocurre en el marco de servidores centrales, no distribuidos, y precisamente por eso, la Justicia puede resolver conflictos con relativa facilidad.

En cambio, en un entorno de smart contracts, ocurre lo siguiente: (i) las partes no se conocen y los IPs de una computadora tampoco permiten conocer la identidad real, (ii) no habrá detalles sobre el objeto vendido, ni la forma de pago empleada si las partes pagan con criptomonedas, sólo se pueden ver transferencias entre llaves públicas, (iii) los contratos se auto-ejecutan de acuerdo a su programación específica, en una red descentralizada y autónoma que no está sujeta a ningún control estatal o jurisdiccional, y por todo ello (iv) no es técnicamente posible la intermediación tradicional de los sistemas jurisdiccionales.

[508]

Idem, p. 47. Ampliar en <https://www.blockchainaragon.com>. Anotando el caso *Aragon*, Kaal y Calcaterra apuntan que: “*The jurisdiction of the Aragon Network is distributed. Specifically, this means the network does not have a localized geographical existence; it is supranational. Therefore, no existing governmental entity has current legal jurisdiction over the regulation of general smart contracts. The Aragon Network’s particular jurisdiction cannot be controlled by any nation-based court for the practical reason that all litigants and judges are anonymous, and so have no determinable national location. Consequently, no political entity will have any practical effect in the governance of general DAOs. The Aragon Network has three primary goals: 1. Provide models for starting well-designed DAOs. 2. Regulate the behavior of these DAOs according to rules decided upon by a dynamically evolving Aragon constitution, which rewards the discovery of potential hacks. 3. Provide a digital jurisdiction for settling contractual disputes in an anonymous and democratic manner.*” Los resaltados son míos.

[509] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 55.

[510] Ampliar en <https://blog.aragon.org/the-aragon-token-sale-the-numbers-12d03c8b97d3/>, disponible al 18/04/2020. Funciona del siguiente modo: “*Whenever a user wishes to dispute the execution of a contract in the Aragon Network, they post a bond (which will be returned if the dispute is decided in their favor) and a brief of their argument. 5 judges who have posted bonds will be randomly selected from all the users of the network. The judges read the litigants’ briefs and issue their judgements. Majority decisions determine the outcome of the dispute. If a judge ruled with the majority, they are rewarded monetarily; if not, they are punished with the loss of their bond. 2 appeals are possible. If either party disagrees with the judgment they may appeal by posting a larger bond with their argument. This opens a prediction market, where any user in the organization may become a judge by posting a bond. The arguments are read and all judges return their verdicts. Again, majority determines the result of the dispute, with rewards or punishments for judges are given based on whether they sided with the successful party. The final appeal is made to a panel of 9 “supreme court” judges comprising the most successful judges in the network. A larger bond is posted by the appellant at each stage to prevent the wasting of system resources.*” El sistema está tan bien pensado, que podríamos utilizarlo en el mundo real...de allí el rotundo éxito en la venta de sus tokens.

[511] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 53.

[512] Confr. Nelson Rodriguez, *¿Qué son los contratos ricardianos? Guía completa*, recuperado el 18/04/2020 en <https://101blockchains.com/es/contratos-ricardianos/>. Los define como una forma de documentos digitales que actúan como un acuerdo entre dos partes sobre los términos y condiciones para una interacción entre las partes acordadas. Lo que lo hace único es que está firmado y verificado criptográficamente. Incluso cuando se trata de un documento digital, **está disponible en un texto legible para personas** que también es fácil de entender para aquellos que no son abogados. Es un acuerdo o documento legal único que se puede leer al mismo tiempo por los programas informáticos y por los humanos, pero **también es un contrato legible para máquinas**. En definitiva, los contratos ricardianos combinan contratos legales con tecnología de la blockchain. Unen a las partes en un acuerdo legal antes de la ejecución de las acciones en la red de blockchain. En contra, Kaal y Calcaterra afirman que “*Because every single Ricardian Contract has an arbiter/notary connected with them to automatically, check the contract, and hold funds in escrow until the contract is validated, such contracts follow the established legal order for contracting to a significant extent.*” El resaltado es mío.

[513] Confr. Stuart D. Levi y Alex B. Lipton, *An introduction to Smart Contracts and their potential and inherent limitations*, recuperado el 18/04/2020 en <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>. Véase también: Ian Grigg, *The Ricardian Contract*, recuperado el 18/04/2020 en https://iang.org/papers/ricardian_contract.html.

[514] Confr. Wulf A. Kaal y Craig Calcaterra, *Crypto transaction dispute resolution*, publicado en *The Business Lawyer*, Primavera 2019, p. 51.

[515] Véase <https://www.openlaw.io>.

[516] Véase *supra* § 1.1.10 en relación al Blockchain 2.0.

[517] Confr. <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>, recuperado el 21/04/2020.

[518] Confr. <https://www.criptonoticias.com/aplicaciones/solardao-y-la-inversion-estable-en-energia-solar/>, recuperado el 16/04/2020.

[519] Confr. <https://daostack.io> recuperado al 27/04/2020.

[520] Confr. <https://wingsfoundation.ch>, recuperado el 22/04/2020.

[521] Confr. <https://cryptoslate.com/coins/xwin-cryptobet/>, recuperado el 21/04/2020.

[522] Confr. <https://decrypt.co/es/25405/piedao-nueva-forma-manejar-fondos-criptomonedas>, recuperado el 15/04/2020.

[523] Confr. Nathaniel Whittemore, *Narrative watch: Why 2020 will be the year of the DAO*, recuperado el 28/04/2020 en <https://www.coindesk.com/narrative-watch-will-daos-break-out-in-2020>. Señala Whittemore casos de DAOs lanzadas en 2019, como MolochDAO (<https://molochdao.com>) y MetaCartel (<https://medium.com/metacartel/metacartel-dao-rises-e0646393718b>).

También señala el autor que las DAOs serán una realidad cada vez más usual, ya que son formas muy flexibles de organizar colectivamente el trabajo de personas interesadas en desarrollar tecnología sobre la base de la CryptoEconomía. Además, las DAOs permiten estructurar nuevas formas de remunerar el trabajo remoto, en un mundo donde el trabajo comienza a transformarse digitalmente a ritmo muy acelerado, y permiten formas mucho más participativas de toma de decisión e inversión.

[524] Confr. José Maldonado, *DeFi: qué es y su impacto en el criptomundo*, recuperado el 01/05/2020 en <https://es.cointelegraph.com/explained/defi-what-it-is-and-its->

[impact-on-the-crypto-world](#).

[525] Confr. <https://makerdao.com/es/>

[526] Confr. Laila Metjahic, *Deconstructing the DAO: the need for legal recognition and the application of Securities Laws to decentralized organizations*, publicado en *Cardozo Law Review*, vol. 39, número 4, disponible al 25/04/2020 en <http://cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf>.

[527] Ibid.

[528] Confr. Shawn Bayern, *Of bitcoins, independently wealthy software, and the Zero-Member LLC*, disponible al 21/04/2020 en <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1009&context=nulr>, p. 1495.

[529] El CCCN, en su Art. 148, define como personas jurídicas privadas a (1) las sociedades; (2) las asociaciones civiles; (3) las simples asociaciones; (4) las fundaciones; (5) las iglesias, confesiones, comunidades o entidades religiosas; (6) las mutuales; (7) las cooperativas; (8) el consorcio de propiedad horizontal; y (9) *toda otra contemplada en disposiciones de este Código o en otras leyes y cuyo carácter de tal se establece o resulta de su finalidad y normas de funcionamiento*.^[LSEP] El resaltado es mío.

[530] Confr. Sebastián Balbín, *Manual de Derecho Societario*, Ed. Abeledo Perrot, Bs. As., 2016, p. 1.

[531] Idem, p. 4.

[532] Idem, p. 5.

[533] Confr. Shawn Bayern, *Of bitcoins, independently wealthy...o.c.*, p. 1495.

[534] Idem, p. 1493, presenta el siguiente ejemplo: “*Suppose that **an independently operating software program**, which we might otherwise have classified as a computer virus, is designed to do something useful, like **perform calculations or store backup copies of data for customers**. Without Bitcoin, there is no legal, convenient way for that software to accept payment from customers unless it does so on behalf of an individual or legal entity, such as a corporation, partnership, or trust. Because of Bitcoin, however, **this program may send and receive valuable digital tokens from anyone on the Internet, and so it can easily act, in functional terms, as an independent business, accepting payment for its services and paying for the resources it uses (such as computer processing and storage) in order to provide them**. It can make these choices as functions of its own software, without ongoing input from humans, and then execute*

the choices using online digital currencies like Bitcoin. Importantly, an independently operating software program could likely do this—practically, very soon in the future, and indeed as a relatively minor engineering challenge—**without special concessions from the law of any jurisdiction**. So long as the inputs to its production are offered online in exchange for bitcoins, the program has no need for conventional financial institutions to pay its operational bills. **So long as its customers are willing to pay the software with bitcoins, it needn't use those institutions to manage its accounts receivable**. Because of advances in computer-networking technology, software can even hide its physical location relatively well, so it might even be difficult to interdict **an autonomous system whose only interaction with the world is to produce and consume digital services** (like storage or information processing) in exchange for bitcoins. Intriguingly, **once a system that provides online services is possible, there is little conceptual barrier to a similar system's providing more conventional "offline" services beyond the Internet**. So, for example, consider a network of vending machines. Someone needs to install the vending machines and continuously supply them. But from the perspective of the software operating the network, those tasks are simply another type of input to production, like disk space or network bandwidth. **The software can pay someone to install or stock a new vending machine, verify that the task has been completed, and remit payment digitally using Bitcoin**. Nothing prevents such services from interacting with each other and assuming a significant economic role.” El resaltado es mío.

[535]

Confr. Reporte de la S.E.C., disponible al 24/04/2020 en <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

[536]

Consultar en <https://slock.it>.

[537]

Confr. Reporte de la S.E.C., p. 1.

[538]

Confr. David J. Shakow, *The Tao of TheDAO: Taxing an Entity that lives on a Blockchain*, recuperado el 28/04/2020 en https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3011&context=faculty_scholarship, p. 931, puntualiza la mecánica de inversiones y retiros: “*The DAO structure allowed persons to transfer Ether (the Ethereum cryptocurrency, similar to bitcoin) to The DAO in exchange for The DAO tokens — items that were ownership interests in The DAO. Token owners voted to choose the investments to be made by The DAO and shared ratably in gains and losses of The DAO and voting was based on the number of DAO tokens owned. Some have questioned whether it might be more democratic if each holder had only one vote. Each token was recorded in the blockchain. The intention was that the collected funds would be invested in start-up companies. A proposal brought to The DAO would be voted on by the holders of The DAO tokens. If enough holders approved of the*

investment, the investment would be made by transferring Ether from The DAO's account to the account of the successful applicant. Those who didn't approve of the investment could choose to take their remaining Ether, leave The DAO's main blockchain and collect their Ether, or create another blockchain. Besides their Ether, those who moved to the new blockchain would also receive "reward tokens." Holders of the reward tokens would receive from The DAO their allocable portion of any distributions that The DAO received from investments made while the members of the new blockchain were still members of the original blockchain of The DAO, and from the proceeds of the disposition of those earlier investments. All of this — the tallying of the votes, the creation of a new blockchain, any distributions to disapproving holders, the investment of funds with successful applicants — could be effected through smart contracts, without the need for human intervention on behalf of The DAO. In its implementation, The DAO also made use of human "curators" who confirmed the identity of those who submitted proposals."

[539]

Confr. Reporte de la S.E.C., p. 9, nota 28.

[540]

Confr. David J. Shakow, *The Tao of TheDAO...o.c.*, p. 932, señala que, como el código del TheDAO –su estatuto social, *mutatis mutandis*– permitía que cualquier inversor se retirara de *TheDAO* si no estaba de acuerdo con una inversión decidida por la mayoría tenedores DAO Tokens –sería el equivalente a un derecho de receso en materia societaria–. El error de programación en el código permitía que se ejercieran estos recesos –i.e. se iniciara un smart contract–, sin que se actualizase el saldo restante del "capital social digital" en Ethers y sin que siquiera hubiera habido una inversión puesta a votación de los inversores que generase la facultad de retirarse. Alguien descubrió el error, y retiró rápidamente DAO Tokens por valor de 3.6 millones de Ethers, que en el momento equivalían a 40 millones de USD. Los DAO Tokens producto de estos "falsos recesos" no eran de libre disponibilidad, sino que quedaban "congelados" por 27 días en una cuenta específica, y luego podían convertirse a Ether, esperando otros 34 días. Se sugiere la lectura directamente de sus fuentes: Dino Mark, Vlad Zamfir y Emin Gür Sirer, *A call for a temporary moratorium on "The DAO"*, recuperado el 15/05/2020 en <https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWys-dQ4lsBacR2dUgGtTV98C40/edit#>.

Confr. Emin Gün Sirer, profesor de la prestigiosa Universidad de Cornell en EE.UU., en *Thoughts on The DAO hack*, recuperado el 01/05/2020 en <https://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/> afirma que: "It's clear that writing a robust, secure smart contract requires extreme amounts of diligence. It's more similar to writing code for a nuclear power reactor, than to writing loose web code.

Yet the current Solidity language and underlying EVM seems designed more for the

latter. Some misfeatures are: (i) A good language for writing state machines would ensure that **there are no states from which it is impossible to recover**. (ii) A good language for writing state machines would make it painfully clear when state transitions can and cannot happen. (iii) A good language for maintaining state machines would **provide features for upgrading the security of a live contract**. (iv) A good language for writing secure code would make it clear that **there are no implicit actions**, that code executes plainly, as read. **The current language does not fulfill any of these commandments, and in fact, the last one, involving implicit recursive calls, is what did The Dao in**. The SlockIt team even had the designer and implementor of Solidity perform a review of their code. If he cannot get something like The DAO to be secure, no one can.” El resaltado es mío.

[541]

Ibid.

[542]

Puede ampliarse en Alex Moskov, *Ethreum Classic vs. Ethereum (ETC vs. ETH): What’s the difference?* Disponible al 20/04/2020 en <https://coincentral.com/ethereum-classic-vs-ethereum/>.

[543]

Confr. Lucy Liu, *The legality of The DAO*, recuperado el 01/05/2020 en <http://mbelr.org/the-legality-of-the-dao/>.

[544]

Confr. Reporte de la S.E.C., p. 11, en el sentido que eran específicamente un contrato de inversión. “**An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others**. See *SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946); see also *United Housing Found., Inc. v. Forman*, 421 U.S. 837, 852-53 (1975) (The “touchstone” of an investment contract “is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.”). This definition embodies a “flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.” *Howey*, 328 U.S. at 299 (emphasis added). The test “permits the fulfillment of the statutory purpose of compelling full and fair disclosure relative to the issuance of ‘the many types of instruments that in our commercial world fall within the ordinary concept of a security.’” *Id.* In analyzing whether something is a security, “**form should be disregarded for substance**,” *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967), “and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto.” *United Housing Found.*, 421 U.S. at 849.” El resaltado es mío.

[545]

Confr. Lucy Liu, *The legality of The DAO...o.c.*

[546] Confr. Laila Metjahic, *Deconstructing the DAO: the need for legal recognition and the application of Securities Laws to decentralized organizations*, publicado en *Cardozo Law Review*, vol. 39, número 4, disponible al 25/04/2020 en <http://cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf>.

[547] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1547.

[548] Confr. Sebastián Balbín, *Manual de Derecho Societario*, Ed. Abeledo Perrot, Bs. As., 2016, p. 424.

[549] Idem, p. 214.

[550] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1562.

[551] Confr. Sebastián Balbín, *Manual de Derecho Societario*, Ed. Abeledo Perrot, Bs. As., 2016, p. 144.

[552] En nuestro derecho, el capital social de las sociedades colectivas se divide en fracciones alícuotas, no necesariamente iguales, llamadas partes de interés, las que no son libremente cesibles. Son embargables las utilidades que correspondan al socio, pero no son ejecutables las partes de interés, debido al carácter esencial del socio colectivo. Confr. Sebastián Balbín, *Manual de Derecho...o.c.* p. 428.

[553] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1552.

[554] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1548.

[555] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1553.

[556] En nuestro derecho, podría sostenerse que *TheDAO* también podría encuadrar como un negocio en participación, regulado en los Arts. 1448 a 1452 del CCCN. Comparar ésta regulación, con la definición de joint venture para el common law: “*Facts showing a pooling of funds or labor with a common purpose to attain a result for the benefit of all the parties, where each participant has a right in some measure to direct conduct, will tend to show a joint venture exists.*” Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1560.

[557] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1561.

[558] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1566, *in re SEC v. Trendon T. Shavers & Bitcoin Savs. & Tr.*, No. 13–CV–416, 2014 WL 4652121 (E.D. Tex. Sept. 18, 2014).

[559] Confr. Laila Metjahic, *Deconstructing the DAO...o.c.*, p. 1564.

[560]

Confr. en este mismo sentido, Lucy Liu, *The legality of The DAO*, recuperado el 01/05/2020 en <http://mbelr.org/the-legality-of-the-dao/>, citando a Reuben Bramanathan, *Blockchains, smart contracts and the Law*, recuperado el 28/04/2020 en <https://blog.coinbase.com/blockchains-smart-contracts-and-the-law-709c5b4a9895>, quien sostiene: “No legal entity is in possession or control of the funds raised, and no legal entity manages the activities of The DAO. **This might mean that the profits of the enterprise are not ‘solely dependent on the efforts of the promoter or a third party’ — because the profitability of The DAO would have depended on all of the token holders voting for profitable things to do with all that ETH.**” El resaltado es mío.

[561]

Confr. Konstantinos Christidis y Michael Devetsikiotis, en *Blockchains and Smart Contracts for the Internet of Things....o.c.*, p. 2298.

[562]

Ibid. Los autores dan interesantes ejemplos del *blockchain-powered IoT devices*: “Consider the following setup to get an understanding of how this could work. All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network. The devices either ship with the smart contract’s address baked into their blockchain client, or they find out about it via a discovery service. They can then query the contract, find out about the new firmware, and request it by its hash via a distributed peer-to-peer filesystem such as IPFS. The first requests for this file will be served by the manufacturer’s own node (also taking part into the network), but after the binary has propagated to enough nodes, the manufacturer’s node can stop serving it. Assuming the devices are configured so as to share the binary they got, a device that joins the network long after the manufacturer has stopped participating in it, can still retrieve the sought- after firmware update and be assured that it is the right file. This all happens automatically, without any user interaction. Compare and contrast with the centralized scenario where the device polls the manufacturer’s server for an update and gets a 404 error. **Furthermore, a blockchain network where cryptocurrency is exchanged provides a convenient billing layer and paves the way for a marketplace of services between devices.** In the example above, devices that store a copy of the binary may charge for serving it, in order to sustain their infrastructure costs (or simply to make a profit). Other examples include: Filecoin which allows devices to “rent their disk space”, and EtherAPIs, which make it possible to monetize API calls – the caller needs to provide the necessary micropayment (in Bitcoin or Ethereum respectively) before requesting them. **With a cryptocurrency in place, every device can have its own bank account on the Internet; it can then expose its resources to other devices (or users) and get compensated for their usage via microtransactions.** This also facilitates the sharing of services and property in general. Slock.it works on smart electronic locks (“Slocks”) that can be unlocked with a device that carries the appropriate token. These tokens are bought on the Ethereum blockchain,

a public blockchain network optimized for smart contracts that uses its own cryptocurrency, called Ether. **The owner of a Slock that wishes to rent their house or car sets a price for timed access to that electronic door lock.** An interested party can use a mobile app to identify the slock, pay the requested amount in Ethers, then communicate with the lock via a properly signed message (using the Whisper peer-to-peer communication protocol) to unlock it. Billing is simplified by having all the Slocks operating on the same blockchain. (...) in the energy sector, **the integration of IoT with blockchains allows for a peer-to-peer market where machines can buy and sell energy automatically, according to user-defined criteria.** For example, TransActive Grid is experimenting with the concept of a peer-to-peer market for renewable energy in a neighborhood in Brooklyn, NY. **Solar panels record their excess output on the blockchain, and sell it to neighboring parties via smart contracts.**” El resultado es mío.

[563]

Confr. Konstantinos Christidis y Michael Devetsikiotis, en *Blockchains and Smart Contracts for the Internet of Things...*o.c., p. 2301.

[564]

Ibid.

[565]

Confr. OpenLaw, *The LAO: A for-profit, limited liability Autonomous Organization*, recuperado el 05/05/2020 en <https://medium.com/openlawofficial/the-lao-a-for-profit-limited-liability-autonomous-organization-9eae89c9669c>.

[566]

Ibid.

[567]

Confr. OpenLaw, *The LAO: A for-profit, limited liability Autonomous Organization*, recuperado el 05/05/2020 en <https://medium.com/openlawofficial/the-lao-a-for-profit-limited-liability-autonomous-organization-9eae89c9669c>.

[568]

Confr. <https://www.coindesk.com/former-polychain-partner-ryan-zurrer-is-leaving-web3-to-start-his-own-dao>, recuperado el 23/04/2020. Puede verse el White Paper de la nueva DAO aquí: <https://github.com/the-dao/whitepaper>, disponible al 23/04/2020.

[569]

Para un análisis general de MolochDAO, véase <https://concourseopen.com/blog/moloch-dao-explained/>, disponible al 25/04/2020. White Paper disponible, en la misma fecha, aquí: <https://github.com/MolochVentures/Whitepaper/blob/master/Whitepaper.pdf>

[570]

Confr. White Paper de Moloch, disponible aquí al 25/04/2020: <https://github.com/MolochVentures/Whitepaper/blob/master/Whitepaper.pdf>

[571]

Confr. Sebastián Balbín, *Manual de Derecho Societario ...*o.c., p. 546 lo define como la potestad conferida al socio por ley o convención estatutaria, para que éste

solicite la extinción del vínculo que lo une con la sociedad, en razón de la ocurrencia de algún supuesto *que altere de manera sustancial su relación originaria con el ente*. Habilita la salida del accionista disconforme, a cambio del reembolso del valor de sus acciones. La Ley General de Sociedades en su Art. 244, último párrafo, enumera nueve causales legales que habilitan el receso, a las que se pueden sumar las causales convencionales que los socios hayan pactado en el estatuto social. El Art. 245 regula el ejercicio del derecho, el que sólo corresponde a los que votan en contra de una resolución asamblearia y a los ausentes, y debe ejercerse dentro de un plazo de 5 o 15 días, según se trate de presentes que votaron en contra, o de ausentes. La sociedad puede celebrar otra asamblea posterior, dentro de los 60 días, para revocar lo decidido e inhabilitar el consecuente receso. Se trata de un derecho que no puede ser renunciado anticipadamente, y está prohibido por la ley agravar las condiciones de su ejercicio, aunque se admite su reglamentación.

[572]

Véase por ejemplo los servicios ofrecidos por: <https://chainsecurity.com/audits/>; <https://quantstamp.com>; https://consensys.net/?utm_source=cryptobrowser.io. Para una descripción sobre el proceso de auditoría de smart contracts, véase Stefan Beyer, *Smart contracts audits – the 12 steps to blockchain security*, recuperado el 22/04/2020 en <https://medium.com/cryptronics/smart-contract-audits-the-12-steps-to-blockchain-security-82543dc383cc>.

[573]

Confr. Christine Vasileva, *Ethereum network not rolled back after DAO hack*, recuperado el 26/04/2020 en <https://bitcoinist.com/ethereum-network-not-rolled-back-after-dao-hack/>.

[574]

Confr. Kapil Gauhar, *Are smart contracts reversible?* recuperado el 22/04/2020 en <https://www.btcwires.com/round-the-block/are-smart-contracts-reversible/>.

[575]

Ampliar en *DelegatedCall: calling another contract function in Solidity*, recuperado el 22/04/2020 en <https://medium.com/coinmonks/delegatcall-calling-another-contract-function-in-solidity-b579f804178c> y en *Contract ABI Specification*, recuperado en la misma fecha de <https://solidity.readthedocs.io/en/develop/abi-spec.html>.

[576]

Confr. *Legal statement on cryptoassets and smart contracts*, recuperado el 22/04/2020 en https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111_1.pdf.

[577]

Confr. <https://www.accordproject.org/news/bsi/>, disponible al 22/04/2020.

[578]

Ibid. En particular, la propuesta de estándar hecha pública por el BSI fija los siguientes objetivos: “a) *defining the necessary taxonomy and form for contracts that*

*are both human-readable and machine-readable; b) providing a universal and extensible technical baseline foundation to aid the development of solutions and software utilising smart legal contracts in a technology agnostic manner to enable compliant implementations and standards to be developed across software platforms and industries; c) providing facts and use cases that demonstrate how smart legal contracts perform and can benefit users, legal professionals and other interested parties; d) establishing a minimum set of requirements for organizations to adopting and develop smart legal contracts; y e) to provide organizations with a technical framework within which to **digitize new or existing legal contracts, connect them to data services, and deploy them across any technology platform (e.g. cloud or a distributed ledger platform)**, including determination of the scope of permissible contract codification.”*

BSI afirma también que “contracts that are expressed only in natural language are unable to adequately respond to events pertaining to the contract that occur in the physical world, as well as on software systems...By contrast, **smart legal contracts include computational components that enable a contract to communicate with software systems and respond to events that occur in the physical world.** For example, a sales contract could calculate a price based upon the delivery status and conditions of goods and generate payment obligations based upon that state. **That contractual state may be used to configure software systems (e.g. performing transfers of digital assets on blockchain systems, raising invoices on accounting systems)** with a significant reduction in the need for resource-intensive external management. Smart legal contracts therefore improve the efficiency of managing contracts throughout their lifecycle, and remove the need to perform redundant data-entry to configure IT systems based on the terms negotiated within the contract. **Moving contracts from purely textual documents, only accessible to humans, to documents containing structured data, accessible to computers, potentially allows contract users to reliably query, extract or integrate contract data with IT Systems.** Smart legal contracts potentially enable contracts to transition from being static records of agreement, to dynamic pieces of IT infrastructure. **Smart legal contracts potentially ensure that all contracting parties have a common view of the state of a contract and all events that might have modified the state of the contract.** Smart legal contracts have an opportunity to create a more efficient way of transacting contractual obligations. The settlement of such obligations, as a baseline, can be done through traditional settlement means. **Distributed ledger technology (DLT) can be used to distribute the state of a contract to the participants in a public or permissioned business network.** Smart legal contracts can potentially remove the need to manually perform contract obligations, such as notification or payment that can often be error-prone and time-consuming manual processes. **Further benefits arise when the settlement of the transacted obligations can happen via settlement native to a specific system (i.e. native tokens) on DLT systems.**” El resaltado es mío.

[579] Véase *infra* nota 752.

[580] Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts templates: foundations, design landscape and research directions*, recuperado el 23/04/2020 en <https://arxiv.org/abs/1608.00771>.

[581] *Idem*, p. 1.

[582] Confr. Pablo Salvador Coderch, *El oficio de la buena prosa legal*, recuperado el 25/04/2020 en <https://indret.com/el-oficio-de-la-buena-prosa-legal/>.

[583] Confr. Christopher Clack, Vikram Bakshi y Lee Braine, *Smart contracts ... o.c.*, p. 6.

[584] *Idem*. Sostienen los autores, p. 7: “Deriving the set of code parameters may be complicated by three factors: (1) **It is common for parameters to be embedded in the legal prose — such parameters would initially be identified visually, aided by a graphical user interface.** (2) Some of the values identified as “parameters” in the agreement (or template) may not have an operational impact and therefore would not be passed to the smart contract code. (3) It is possible for a parameter to be defined (given a name) in one document, given a value in a second document, and used (e.g. in business logic) in a third document. Although parameters need not have values in a template, they must have values in a signed agreement. All of an agreement’s parameter values are a critical part of the contract as they directly reflect the business relationship between parties and those that are code parameters influence the automated operation of the contract. Most parameters in existing templates have simple types, such as date, number, etc. These are “base” or “primitive” types. It is not necessary for parameters to be restricted to base types. It is very likely that values of more complex types, such as lists, will also need to be transferred to the code. **The passing of parameters to the code is necessary because of the desire to use standardised code.** The number of parameters, and the complexity of the types of those parameters, will typically increase as the code becomes more generic. Beyond parameters with base types and more complex types such as lists, **parameters can also be expressions containing references to other parameter names.** Unless those other parameter names are defined within the expression, the expression is effectively a function. **Where a function is passed as a parameter, this is known as a “higher-order” parameter and the receiving code is known as a “higher-order” function.**” El resaltado es mío.

[585] *Idem*, p. 9.

[586] *Ibid.*

- [587] La EFF se dedica a defender las libertades civiles en el mundo digital. Véase: <https://www.eff.org/es/pages/acerca-de-eff>.
- [588] Disponible al 23/04/2020 en <https://www.eff.org/es/cyberspace-independence>.
- [589] Ibid.
- [590] Véase *supra* § 1.1.5.
- [591] Confr. Lawrence Lessig, *Deja vú all over again: thinking through law & code, again*, conferencia brindada en el *Sidney Blockchain Workshop*, Diciembre de 2015. Video disponible al 01/04/2020 en <https://www.youtube.com/watch?v=pcYJTlBhYF0>
- [592] Confr. Kevin Werbach, *The song remains the same: what cyberlaw might teach the next Internet economy*, o.c. p. 887.
- [593] Confr. Aaron Wright y Primavera De Filippi, *Decentralized...* p. 50.
- [594] Confr. Kevin Werbach, en *Trustless Trust...* o.c. p. 58.
- [595] Ibid.
- [596] Confr. Karen Yeung, en *Regulation by blockchain..* p. 218, nota 45.
- [597] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 528.
- [598] Ibid.
- [599] Véase https://es.wikipedia.org/wiki/Ross_Ulbricht.
- [600] Véase <https://es.cointelegraph.com/news/alexander-vinnik-claims-injustice-while-now-fighting-charges-in-france>, disponible al 24/04/2020.
- [601] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 529.
- [602] Idem, p. 534.
- [603] Confr. Intal-BID, *Algoritmolandia: Inteligencia Artificial para una integración predictiva e inclusiva de América Latina*, Ed. Planeta, 2018, Bs. As., p. 10.
- [604] Confr. Karen Yeung, en *Regulation by blockchain..* p. 215.
- [605] Idem., p. 216.
- [606] Idem., p. 220.
- [607] Idem., p. 218. Afirma Yeung que si bien las primeras medidas y acciones han

sido contra intermediarios, fácilmente identificables por actuar como “puertas de ingreso” entre el mundo real y el entorno blockchain, *“as the need for intermediaries evaporates, as more services are placed on unpermissioned blockchains, national legal systems might seek to target and impose legal responsibilities on code developers and miners directly; although whether they can do so successfully in practice will, at least for the time being, remain unanswered.”* (el resaltado es mío).

[608] Ampliar en Tristan Pollock, *Silk Road was the fastest growing online marketplace ever*, recuperado el 25/04/2020 en <https://medium.com/startup-grind/silk-road-was-the-fastest-growing-online-marketplace-ever-be5759ab3332>.

[609] Ibid.

[610] Ibid.

[611] Confr. https://elpais.com/internacional/2015/05/29/actualidad/1432935074_571369.html, recuperado el 26/04/2020.

[612] Confr. <https://es.cointelegraph.com/ripple-101/what-is-ripple>, recuperado al 01/05/2020.

[613] Confr. <https://zycrypto.com/xrp-to-hit-50-if-ripple-grabs-10-of-swifts-market-share/>, recuperado el 30/04/2020.

[614] Confr. <https://www.crypto-news-flash.com/es/swift-esta-probando-la-tecnologia-de-ripple-para-el-procesamiento-de-pagos/>, recuperado el 30/04/2020.

[615] Confr. comunicado de prensa, <https://www.fincen.gov/sites/default/files/shared/20150505.pdf>, recuperado el 30/04/2020.

[616] Ibid.

[617] Ibid.

[618] Véase *supra* § 1.1.9.1.1.

[619] Confr. Adrian Zmudzinski, *China’s crackdown on Cryptocurrency trading: a 2019 recap*, recuperado el 22/04/2020 en <https://cointelegraph.com/news/chinas-crackdown-on-cryptocurrency-trading-a-2019-recap>.

[620] Confr. David Pan, *China’s Congress passes cryptography law, effective Jan. 1, 2020*, recuperado el 25/04/2020 en <https://www.coindesk.com/chinas-congress-passes-cryptography-law-effective-jan-1-2020>.

[621] Confr. PwC, *New chinese cryptography law in force as of 1 January 2020*, recuperado el 24/04/2020 en <https://www.pwclegal.de/datenschutz/new-chinese-cryptography-law-in-force-as-of-1-january-2020/>.

[622] Confr. Karen Yeung, en *Regulation by blockchain..* p. 220.

[623] Idem, p. 220, nota 56.

[624] Confr. <https://www.r3.com/press-media/illinois-becomes-first-state-level-regulator-to-join-r3-distributed-ledger-group/>, recuperado el 12/04/2020.

[625] Véase, Richard Gendal Brown, *The Corda Platform: An Introduction*, recuperado el 03/05/2020 en <https://www.corda.net/content/corda-platform-whitepaper.pdf>, y el website: <https://www.r3.com/press-and-media/>.

[626] Confr. Nick Avramov, *How R3 Corda works*, recuperado el 22/04/2020 en <https://medium.com/@nickavramov/how-r3-corda-works-24d9285059a2>.

[627] Confr. <https://www.coindesk.com/over-50-banks-firms-trial-trade-finance-app-built-with-r3s-corda-blockchain>, recuperado al 26/04/2020.

[628] Confr. Karen Yeung, en *Regulation by blockchain..* p. 222.

[629] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 535.

[630] Idem, p. 537.

[631] Idem, p. 538. Véase: <https://open-music.org>.

[632] Confr. Alexander Attar, *The UJO platform: A Decentralized Music Ecosystem*, recuperado el 24/04/2020 en <https://blog.ujomusic.com/the-ujo-platform-a-decentralized-music-ecosystem-e530c31b62bc>.

[633] Puede ampliarse el concepto en Arjun Balaji, *A simple explanation of Crypto-Collectibles*, recuperado el 26/04/2020 en <https://medium.com/crypto-simplified/a-simple-explanation-of-crypto-collectibles-8674c4527bd1>, quien los define como un objeto escaso, de colección digital: “A crypto-collectible is a **cryptographically unique, non-fungible digital asset**. Unlike cryptocurrencies, which require all tokens to be identical, each crypto-collectible token is unique or limited in quantity. Typically, crypto-collectibles are visualized as real-life objects such as pets or avatars. Each token has variations in specific attributes and there are limits to the number of tokens that can be generated.”

[634] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 536.

[635] Confr. Qiuyun Shang y Allison Price, *A blockchain-based land titling Project in the Republic of Georgia*, disponible al 25/04/2020 en https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00276.

[636] Confr. Luis Esparragoza, *Registro inmobiliario de Brasil realizará prueba con blockchain para registrar títulos de propiedad*, recuperado el 28/04/2020 en <https://www.criptonoticias.com/comunidad/adopcion/registro-inmobiliario-brasil-realizara-prueba-blockchain-registrar-titulos-propiedad/>.

[637] Confr. Romina Monteverde, *Brasil es el primer país del mundo en emitir certificados de nacimiento en blockchain*, recuperado el 01/05/2020 en <https://www.tekcrispy.com/2019/09/02/brasil-emitir-certificados-nacimiento-blockchain/>.

[638] Confr. Karen Yeung, en *Regulation by blockchain..* p. 222.

[639] Idem, p. 225.

[640] Se recomienda la lectura del excelente artículo de Alina Myalo, *Comparative Analysis of ICO, DAOICO, IEO and STO. Case Study*, recuperado el 28/04/2020 en https://www.researchgate.net/publication/338154650_Comparative_Analysis_of_ICO

[641] Confr. Karen Yeung, en *Regulation by blockchain..* p. 226.

[642] Confr. A. S. Myalo, *Comparative Analysis of ICO, DAOICO...o.c.*, p. 8, precisa: “As a rule, the White Paper should contain the following sections: 1) the description of a business idea or a problem; 2) the proposed solution and the description of the relevant project/product; 3) the description of a token implementation mechanism (how it interacts with the product, economy, and its technical implementation); 4) the Project team; 5) the parameters and timing of the release of tokens, the plans for future. The procedure for issuing an ICO is usually the following: A. Pre-ICO launch — pre-sale of units of a new currency, usually at a reduced price, compared to the one that will be at the first moment of selling an ICO. 2. ICO launch — immediate launch of the initial coin offering. Most purchases are made by investors who plan to resell the currency after its value has increased over time.”

[643] La Ley de Mercado de Capitales N° 26.831 regula el prospecto de emisión en sus Arts. 119 a 124. Todos los firmantes de un prospecto asumen responsabilidad solidaria, con posibilidad de determinar una participación personal en el monto a indemnizar, en función del grado de acceso efectivo a la información. Las Normas de la C.N.V., T.O. 2013 precisan su contenido en el Título II, Capítulo IX.

[644] Confr. A. S. Myalo y N. Yu Glukov, *Factors of success of Initial Coin Offering*.

Empirical evidence from 2016-2019, recuperado el 26/04/2020 de https://www.researchgate.net/publication/336792445_Factors_of_Success_of_Initial_Coin_Offering_2019, p. 33.

[645]

Confr. <https://www.statista.com/statistics/802925/worldwide-amount-cryptocurrency-ico-projects-by-industry/>, recuperado el 26/04/2020.

[646]

Confr. Toju Ometoruwa, *ICOs issued \$24.2 billion in tokens to themselves in 2018, where did it all go?* Recuperado el 25/04/2020 en <https://cryptopotato.com/icos-issued-24-2-billion-in-tokens-to-themselves-in-2018-where-did-it-all-go/>.

[647]

Desde el 8 de Enero de 2018 al 16 de Diciembre de 2018, el cryptomarket perdió el 87.75% de su valor, pasando de un mercado de 833.000 millones de Dólares a uno de 102.000 millones de Dólares. Confr. <https://www.hiveex.com/cryptocurrency-landscape-statistics-report-2019>, recuperado el 17/04/2020.

[648]

Ibid.

[649]

Confr. A. S. Myalo y N. Yu Glukov, *Factors of success of...o.c.* p. 39.

[650]

Confr. OECD, *Initial Coin Offerings (ICOs) for SME financing*, recuperado el 25/04/2020 en <https://www.oecd.org/finance/ICOs-for-SME-Financing.pdf>, p. 7.

[651]

Confr. A. S. Myalo, *Comparative Analysis of ICO, DAOICO, IEO and STO. Case Study*, recuperado el 28/04/2020 en https://www.researchgate.net/publication/338154650_Comparative_Analysis_of_ICO p. 8, afirma que los fraudes en ICOs, según Satis Group, alcanzarían al 81% de todas los ICOs; un 11% no tuvo éxito por razones de negocio, y sólo un 8% llegó a completar el proyecto fondeado de manera exitosa. Los ataques cibernéticos, por su parte, son también muy frecuentes, y hasta el 10% de los fondos recaudados vía ICOs fueron robados por cibercriminales. También se señala que existe un alto riesgo fiscal, además de regulatorio.

[652]

Confr. Karen Yeung, en *Regulation by blockchain..* p. 230.

[653]

El término *soft law* ha sido acuñado en el ámbito del Derecho Internacional Público, pero luce muy aplicable a entornos digitales *on-chain*. *Soft law*, en ese contexto, hace referencia a

“[...] normas que se encuentran en proceso de formación y aun no han adquirido validez jurídica. [...] normas jurídicas de contenido vago o difuso en las que resulta difícil precisar si sus disposiciones han sido o no cumplidas debidamente. [...] normas que se hallan en resoluciones de la Asamblea General de las Naciones Unidas, [...] en los acuerdos políticos entre los gobiernos [...]”, confr. Alan Matías Feler, *Soft law como herramienta de adecuación del Derecho Internacional Público a las nuevas coyunturas*,

recuperado el 26/04/2020 en <http://www.derecho.uba.ar/publicaciones/lye/revistas/95/soft-law-como-herramienta-de-adequacion-del-derecho-internacional-a-las-nuevas-coyunturas.pdf>, p. 288.

[654]

Confr. Karen Yeung, en *Regulation by blockchain..* p. 239.

[655]

Véase Sebastián Heredia Querro, *Token Economics y Corporate Finance: Tensiones entre las regulaciones bursátiles del Siglo XX y la tecno-democratización del acceso al financiamiento en el Siglo XXI*, publicado en Diario La Ley, Miércoles 10/07/2019.

[656]

El *Cryptoeconomics Lab* del MIT es un buen lugar para empezar a entender qué significa Token Economics. Sin embargo, ninguna de las definiciones que uno puede revisar logra imponerse por simpleza y claridad, por lo cual optaré por esbozar una propia combinando ideas ajenas, todas gestadas al amparo del MIT, y diseccionando el aspecto tecnológico del fenómeno (i.e. tokenización) del aspecto económico. Como primera aproximación, más tecnológica, puede sostenerse que esta disciplina estudia cómo se diseñan, fundeán, desarrollan, promueven y operan plataformas digitales descentralizadas, y los bienes y servicios digitales en ellas tranzados.

Como segunda aproximación, más económica, la disciplina estudia los medios por los cuales la blockchain puede reducir costos de verificación –de ciertos atributos de una transacción– y de trabajo en red –operando en plataformas digitales descentralizadas sin necesidad de recurrir a un tercero de confianza–, con doble foco en la utilización de tokens que viabilizan el intercambio seguro información o valor entre las partes de la red y en cómo impactan los efectos de red en esta nueva tecnología.

Los Profesores Christian Catalini (MIT Sloan School of Management) y Joshua Gans (Universidad de Toronto) en un reciente paper titulado *Initial Coin Offerings and the value of Crypto Tokens*, disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213 al 25/04/2020, proponen una tesis interesante y, sin dudas, muy polémica: en determinados supuestos, la emisión de Utility Tokens que permiten acceder/transaccionar en una determinada plataforma/servicios, permiten captar fondos *de forma más eficiente* que fondeando el emprendimiento emitiendo acciones, siempre y cuando el emprendimiento se obligue a emitir una cantidad limitada de tokens, y obligue a pagar sólo con dichos tokens por el uso/acceso/transacciones entre el tenedor del token y el emprendimiento así fondeado. Consideran los autores que este mecanismo de fondeo funciona adecuadamente solo en *early stage*, y es conveniente captar posteriormente fondos adicionales (*follow-on investments*) a través de acciones. Señalan también los autores que la práctica actual de los fondos *Venture Capital* muestra negocios híbridos, donde se capitalizan emprendimientos a cambio tanto de acciones como de tokens, debido a la incertidumbre futura sobre qué tendrá más valor, si el token o una acción del emprendimiento.

[657] Disciplina integrante de la ciencia de las Finanzas, que estudia cómo se financian las empresas, cómo se estructura su balance, y cómo tomar decisiones de inversión y cobertura bajo una óptica de maximización de la creación de valor sustentable para los propietarios de la empresa.

[658] Para un análisis de un caso reciente de abuso/fraude bursátil, véase del autor: “*Reflexiones sobre derivados sintéticos: la postura de la SEC en el caso Goldman Sachs*”, Eldial.com, Supl. Dcho. Empresario, Junio 2010. En materia de abusos vinculados *insider trading*, véase del autor “*El uso de información privilegiada en el mercado de acciones y la acción de responsabilidad*”, ponencia en co-autoría con los Dres. Leopoldo Godio y Sebastián Vanella Godino, presentada al I Congreso Argentino Sobre Mercado de Capitales, Aspectos Jurídicos y Contables, organizado por UCEMA, publicada en Mercado de Capitales, Aspectos Jurídicos y Contables, Dto. de Finanzas UCEMA, Ed. Osmar D. Buyatti, 2008, págs. 395-409.

[659] Por todas, ver <https://www.iosco.org/publications/?subsection=ico-statements> disponible al 28/04/2020.

[660] Disponible al 28/04/2020 en <https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1204/1204-alerta-al-publico-inversor-sobre-ofertas-iniciales-de-monedas-virtuales-o-tokens>.

[661] Confr. Ley 27.430, B.O. 29/12/2017, Art. 2.

[662] Comunicado del 18/01/18, disponible al 28/04/2020 en <https://www.iosco.org/news/pdf/IOSCONEWS485.pdf>

[663] Disponible al 28/04/2020 en <https://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf>

[664] Confr. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/> disponible al 26/04/2020.

[665] Confr. <https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf> disponible al 27/04/2020.

[666] Disponible en <https://coincenter.org/files/2019-03/clayton-token-response.pdf> al 27/04/2020.

[667] Confr. <http://www.thetechnolawgist.com/2019/03/13/la-sec-se-pronuncia-sobre-la-naturaleza-juridica-de-los-tokens-digitales/> disponible al 24/04/2020.

[668] Véase *supra*, § 2.6.1.1. En esencia, para la SEC un *Token* será considerado un contrato de inversión, y por ende un *Security* sujeto a su competencia regulatoria en

función de los hechos y circunstancias concretas, especialmente la realidad económica de la transacción, y su encuadre en las leyes de 1933 y 1934 (Siglo XX, por cierto), y jurisprudencia de la Corte Suprema en los casos Howey (1946) y Forman (1975, también del Siglo XX). Para la SEC, existirá contrato de inversión que habilita su competencia cuando existe una inversión en un emprendimiento común, basada en una expectativa razonable de obtener ganancias producidas por el esfuerzo de gestión de otros. “Entrepreneurial or managerial efforts of others” son las palabras clave.

[669] Confr. <https://www.congress.gov/bill/116th-congress/house-bill/2144> disponible al 25/04/2020.

[670] Texto propuesto en inglés: “DIGITAL TOKEN.—*The term ‘digital token’ means a digital unit—“(A) that is created— “(i) in response to the verification or collection of proposed transactions; “(ii) pursuant to rules for the digital unit’s creation and supply that cannot be altered by any single person or persons under common control; or “(iii) as an initial allocation of digital units that will otherwise be created in accordance with clause (i) or (ii); “(B) that has a transaction history that— “(i) is recorded in a distributed, digital ledger or digital data structure in which consensus is achieved through a mathematically verifiable process; and “(ii) after consensus is reached, resists modification or tampering by any single person or group of persons under common control; “(C) that is capable of being transferred between persons without an intermediate custodian; and “(D) that is not a representation of a financial interest in a company or partnership, including an ownership interest or revenue share.”*

[671] Texto propuesto en inglés: “IN GENERAL.—**No law, rule, regulation, or order, or other administrative action** of any State or any political subdivision thereof—“(A) requiring, or with respect to, registration or qualification of securities, or registration or qualification of securities transactions, **shall directly or indirectly apply to a digital token**; “(B) shall directly or indirectly prohibit, limit, or impose any conditions upon the use of— “(i) with respect to a digital token, any disclosure document concerning an offer or sale of a digital token that is prepared by or on behalf of a person developing, offering, or selling a digital token; or “(ii) any proxy statement, report to digital token-holders, or other disclosure document relating to a digital token or a person developing, offering, or selling a digital token; “(C) shall directly or indirectly prohibit, limit, or impose conditions, based on the merits of a digital token offering or a person developing, offering, or selling a digital token, upon the offer or sale of any digital token; or “(D) shall directly or indirectly require the filing of any notices or other documents, or the assessment of any fees, with respect to digital tokens or digital token transactions. (2) PRESERVATION OF FRAUD AUTHORITY.—*States and political subdivisions thereof shall retain jurisdiction under the laws of such State to investigate and bring enforcement actions with respect to fraud or deceit, or unlawful conduct by any person, in connection with digital tokens or digital token transactions.*” El resaltado es mío.

[672] Confr. A. S. Myalo, *Comparative Analysis of ICO, DAOICO, IEO...* o.c. p. 14.

[673] Ampliar en Iliya Zaki, *Security Token Offerings (STOs) – what you need to know*, recuperado el 29/04/2020 en <https://hackernoon.com/security-token-offerings-stos-what-you-need-to-know-8628574d11e2>.

[674] Ibid.

[675] Confr. Syed Shoeb, *Will 2019 be the year of the STO?* Recuperado el 29/04/2020 en <https://hackernoon.com/will-2019-be-the-year-of-the-sto-understanding-stos-security-tokens-market-potential-over-icos-4d2502227220>. Ampliar en Aashish Sharma, *Will STOs (security token offerings) rule over ICOs in 2019*, recuperado el 30/04/2020 en <https://hackernoon.com/will-stos-security-token-offerings-rule-over-icos-in-2019-8feda7bcf562>.

[676] Ibid.

[677] Confr. CoinDesk, *Security Token Offerings are (finally) set for takeoff in 2020*, disponible el 28/04/2020 en <https://www.coindesk.com/security-token-offerings-are-finally-set-for-takeoff-in-2020>.

[678] Confr. Marko Vidrih, *Simple Agreement for Future Token (SAFT) – Explained*, recuperado el 22/04/2020 en <https://medium.com/the-capital/simple-agreement-for-future-tokens-saft-explained-a72d23cddf77>. Véase también *The SAFT project: toward a compliant token sale framework*, disponible al 30/04/2020 en <https://www.crowdfundinsider.com/wp-content/uploads/2018/03/SAFT-Project-Whitepaper-October-2017.pdf>.

[679] Confr. *The SAFT project: toward a compliant token sale framework*, o.c. donde se indica que: “The resulting tokens, however, are already functional, and need not be securities under the Howey test. They are consumptive products and, as such, demand compliance with state and federal consumer protection laws.” Afirman el punto sosteniendo que “Ultimately, not every already-functional utility token will fail the Howey test. For these tokens, using a SAFT will not aid in navigating the securities laws. Howey is not a black-and-white metric for security status. It is a highly variable facts-and-circumstances test. **Some utility tokens, due to their particular facts or circumstances, may pass the Howey test despite being already-functional**”. El resaltado es mío.

[680] Ampliar en <https://www.ycombinator.com/documents/>, disponible al 28/04/2020.

[681] Confr. Marko Vidrih, *Simple Agreement for Future Token (SAFT) –*

Explained...o.c. p. 1 afirma:

“Other token sales happen long before the token network has genuine functionality; so-called “direct token pre-sales” are sold at greater discounts with the goal of financing the development of the network and its launch. **Purchasers in these direct presales tend to expect profit predominantly from the seller’s efforts to create functionality in the token.** As such, these sellers may unintentionally be selling securities, and may have failed to comply with several U.S. laws. “El resultado es mío.

[682]

Confr. Marko Vidrih, Simple Agreement for Future Token (SAFT) – Explained...o.c. p. 1

[683]

Confr. David Felsenthal y Jesse Overall, Bad news: SAFTs may not be “Compliant” after all, recuperado el 01/05/2020 en <https://www.crowdfundinsider.com/2018/03/130229-bad-news-safts-may-not-compliant/>. Sostienen los autores que:” The SAFT itself is a security. It is a contract giving the purchaser the right to receive the issuer’s tokens that will be issued in the future, and is sold to accredited investors in a Rule 506(c) private offering, for which the issuer files a Form D. The issuer then uses the proceeds raised by the SAFT sale to finance the development of its software network. Once development is completed, **the issuer issues and delivers now fully-functional utility tokens, useable on its network, to the original SAFT holders. SAFT proponents argue that the tokens are not securities and therefore purchasers can freely re-sell the utility tokens to retail investors without being deemed to have facilitated an unregistered securities offering,** acted as unregistered broker-dealers or violated mandatory holding *periods*, while intermediaries – such as trading platforms listing such tokens for trading – would not have an SEC registration obligation.” En esencia, se comparte la calificación jurídica que subyace en un SAFT, pero su verdadera utilidad se ve afectada si los tokens a emitirse son tratados como Security Tokens aún cuando sean claros ejemplos de Utility tokens.

[684]

Confr. Cardozo Blockchain Project, *Not so fast – risks related to the use of a “SAFT” for token sales*, recuperado el 24/05/2020 en <https://www.crowdfundinsider.com/wp-content/uploads/2017/11/Cardozo-Blockchain-Project-Not-So-Fast-SAFT-Response.pdf>.

[685]

Distintos casos tristemente célebres de ICOs pueden verse en Shankar Iyer, *Crypto Scams: an advanced guide to cryptocurrencies*, recuperado el 23/04/2020 en <https://marketrealist.com/2020/01/crypto-scams-an-advanced-guide-to-cryptocurrencies/>.

[686]

Confr. A. S. Myalo, *Comparative Analysis of ICO, DAOICO, IEO...*o.c. p. 9.

[687]

Idem, p. 13.

[688] Confr. <http://cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf> disponible al 27/04/2020.

[689] Ampliar en <https://www.fca.org.uk/firms/regulatory-sandbox>, disponible al 29/04/2020.

[690] Confr. <https://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/220219-enlacedigital.aspx> disponible al 29/04/2020.

[691] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based token sales, initial coin offerings, and democratization of public capital markets*, disponible al 25/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104. Citado con el permiso de los autores.

[692] Criterio que ha sido mantenido en 2017 en los casos Munchee y Plexcorps, y en 2018 en el caso Arisebank. Confr. <https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf>, recuperado el 26/04/2020. En Arisebank, la SEC afirmó que la appcoin, AriseCoin, era una ICO ilegal, al no estar previamente registrada en la SEC; habiendo oferta pública por medios masivos de comunicación en Internet.

[693] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based...o.c.* p. 10.

[694] Idem, p. 14.

[695] Idem, p. 19.

[696] Idem, p. 21.

[697] Idem, p. 22. Afirman los autores que, tomando como muestra el mes de Marzo de 2017, el 75% de los tokens vendidos conferían un derecho de acceso o uso de servicios digitales; y el 50% utilizaba el token como mecanismo de pago. Los derechos de voto, o a participar del resultado de la inversión fueron poco comunes, y se encontraron presentes en el 25% de los tokens emitidos.

[698] Véase <https://status.im/es/snt-utility/>.

[699] Véase <https://blog.bitso.com/te-desespera-ver-anuncios-en-internet-conoce-basic-attention-token-bat-9cba03440c69>, recuperado el 26/04/2020.

[700] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based...o.c.* p. 24.

[701] Véase <http://securitytokencap.io/currency/blockchaincapital>, y

<https://sharespost.com/insights/research-reports/10-things-you-should-know-about-blockchain-capitals-bcap-security-token-preview/>, recuperado el 26/04/2020.

[702] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based...* o.c. p. 26.

[703] Idem, p. 27, nota 72.

[704] Idem, p. 28, nota 77.

[705] Excepto para los tokens que normalmente retiene para sí el equipo desarrollador, los que suelen estar *vesteados*, es decir, tienen prohibición de transferencia hasta que ocurren hitos o se cumplen determinados plazos. Un esquema usual de Founder Vesting Agreement es el siguiente: “*Founders will have 2 years vesting with 6 months cliff. This means we will mature 25% of our tokens each 6 months. Early contributors, presale partners and advisors will have 6 months vesting with 3 months cliff. This means they will mature 50% of their tokens at the end of month #3, and the rest on month 6*”. Idem, p. 29, nota 78.

[706] Idem, p. 29.

[707] Idem, p. 34, comentan el caso del Golen Token, que de un precio inicial de \$0.015 por token, llegó a valer \$1.25, es decir, un incremento del 9.120%. Citan también el caso de DigixGlobal, con su Token DGX, que en menos de un año pasó de valer \$6 a \$350.

[708] Idem, p. 31.

[709] Idem, p. 32, donde señalan varios casos donde el 80% de los app tokens vendidos fueron comprados por solo 10-100 inversores.

[710] Idem, p. 34.

[711] Idem, p. 37.

[712] Idem, p. 39.

[713] Con lo cual estos tokens quedan sujetos a las normas dispuestas por la Ley de Securities de 1933 y la ley de la S.E.C. de 1934, y deben ser previamente registrados para poder ser ofrecidos públicamente a los inversores. La primera ley se aplica si existe un security, y para determinar su existencia se aplica el concepto de contrato de inversión desarrollado en el caso *Howey*, decidido por la Corte Suprema de EE.UU en 1946, que analiza si existen o no tres características en la emisión: *investment of money, common Enterprise* y *expectation of profit from efforts of others*. Éste último requisito no se cumple si (i) un inversor tiene por intención el uso o consumo de un bien o servicio subyacente, o (ii) se involucra en la gestión gerencial del

empresarial, es decir si es un inversor activo, y no pasivo; ambos factores deben analizarse en cada caso particular.

In re “Rice v. Braniger Organization, Inc., 922 F.2d 788, 791 (11th Cir. 1991) (holding that purchases of lots and memberships in adjacent country club were not securities); Libaire v. Kaplan, 2008 WL 794973 (E.D.N.Y. 2008) (holding that purchase of share in a corporation that operated a private hunting reserve did not involve a security because the purchase was motivated by a desire to access the facility).”

Mismo holding en “*United Housing Foundation, Inc. v. Forman*” decidido por la Corte Suprema: 421 U.S. 837 (1975).

En relación al último requisito del Howey test, agregan los autores que: ***“some utility tokens allow their holders to participate in certain decisions related to the enterprise, and it is conceivable that such participation, if sufficiently extensive, could call into question the security status of the token. The point at which participation by token holders will take the enterprise outside of the definition of security (because the relevant efforts are no longer efforts of others) is only visible with hindsight. Variation in the voting and participation rights extended to token holders is another issue that prevents categorical determinations as to the security-status of utility tokens...Even in the case of investment tokens, the “efforts of others” prong may also lead to differing, and possibly counterintuitive results. Because these tokens may give their holders rights to participate in managerial decision making, some investment tokens may not ultimately qualify as securities even though the expectation of profits is express...An investment token that gives its holders sufficient control or participation rights may be more akin to an interest in a general partnership or joint venture than a security.”*** El resaltado es mío. Idem, p. 51, 63, 67 y 69, notas 138, 139, 163 y 164.

[714] Idem, p. 44.

[715] Idem, p. 52.

[716] Idem, p. 53.

[717] Idem, p. 61. Indican los autores citados que ***“Tokens that are either immediately functional or which will be in a relatively short amount of time after sale seem to offer purchasers a stronger interest in consumption than tokens that will not have any actual use for several months.”*** El resaltado es mío.

[718] Idem, p. 62.

[719] El Art. 4(a)(2) de la ley de Securities de 1933 dispone que existe una excepción si no existe oferta pública. Lo contrario ocurre en la venta de tokens, masivamente publicitadas.

La Regulation D ofrece otras dos excepciones: (i) Regla 504: si la emisión es menor a 5 millones de Dólares, puede ser ofrecida a cualquier tipo de inversor; (ii) Regla 506: no

tiene límite de emisión, pero los inversores deben ser calificados, y si no lo fueran, no podrán ser más de 35. En ambos casos, se prohíbe la reventa del título valor exceptuado dentro del año de compra, sin que sea previamente registrado en la SEC.

La Regulación A+ permite emisiones hasta 50 millones de Dólares, no hay limitaciones a la reventa, pero el emisor debe presentar a la SEC información muy similar a la requerida para una IPO. Si la emisión es de hasta 20 millones de Dólares, puede ser ofrecida a cualquier tipo de inversor, y no hay límites en la cantidad de inversores. Si la inversión es mayor, pero menor a 50 millones de Dólares, aplica un límite a la inversión respecto de inversores no calificados, en función de sus ingresos netos.

Finalmente, la última excepción es la Regulación Crowdfunding, que permite vender hasta 1.070.000 millones de Dólares en securities, en un plazo de 12 meses, pero estas compras están sujetas a restricciones a la transferencia.

[720] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based...* o.c. p. 90.

[721] Véase Monetary Authority of Singapore, *A guide to digital token offerings*, recuperado el 26/04/2020 en <https://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%2>

[722] Confr. Aaron Wright y Jonathan Rohr, *Blockchain-based...* o.c. p. 95.

[723] Idem, p. 97.

[724] Idem, p. 99.

[725] Idem, p. 101, afirman que: “*For a utility token to fall outside the boundaries of federal securities law, the token should be needed to coordinate activity on the application, solve a technical problem, or entitle the user to receive some sort of benefit in the context of the online platform or application. There should be a consumer benefit, and the more dependent operation of the application is on tokens and the participation of token holders, the clearer the interest in consumption is. Tokens sold for applications that can be operated without the token, for example, would appear to offer a less significant interest in consumption than tokens sold for an application that is simply not available unless the user has a token. This type of approach should keep the mere fact that resale is possible from causing all utility tokens to be treated as securities, while also providing a flexible approach to address token sales that attempt to evade their obligations under the securities laws.*”

[726] Idem, p. 102, afirman que “*analysis should focus on extrinsic factors relating to: (1) the manner in which the token sale is marketed and the audience toward which marketing efforts are directed; (2) the ability of the token seller to disproportionately or materially impact the value of the token both before and after the sale; and (3) to a lesser*

degree, whether a token—at the time of sale—can be used within a technological system. For blockchain-based tokens to avoid the ambit of federal securities laws, **any marketing material prepared by the selling party should not contain express or implied indications that the value of the token will appreciate in value and token sellers should not take affirmative steps to market and sell their tokens to sophisticated investors, venture capital funds, crypto hedge funds, and other investors that have no intent to use or consume the underlying good or service.** In much the same way, formal waivers or other agreements whereby token purchasers **affirmatively acknowledge that they are not purchasing the token for speculative purposes** should be factored into a Howey analysis. These agreements represent affirmative efforts on the part of the token seller to control and manage the expectations of token purchasers and sets an objective baseline for evaluating a purchaser's expectation.” (el resaltado es mío)

[727]

Idem, p. 104, lo exponen así: “if a seller takes steps to list a token in regulated U.S. marketplaces prior to, during, or shortly after the sale or **fails to impose transfer restrictions on tokens issued to the developers** or organizations developing the tokens, it indicates that the selling party may be prioritizing the speculative aspects of the token over their consumptive aspects and suggests that the token is an investment opportunity. **The same rationale applies to token distribution structures where sellers “burn” tokens or otherwise try to manipulate the scarcity of the underlying asset.** These acts signal to purchasers that the sellers or organizers will be involved directly in non-operational efforts to manage the value of the tokens, **in the same way that executives of traditional companies undertake share buy-backs** and other transactions to manage the price of publicly traded equity securities.” (el resaltado es mío)

[728]

Idem, p. 113.

[729]

Idem, p. 107. Proponen: “the safe harbor should be designed in a fairly straightforward manner, **insulating compliant exchanges from liability for facilitating the sale of unregistered securities**, provided they took certain steps prior to listing the token and take immediate steps to delist the token if it is subsequently found to be a security. Possibilities for pre-listing actions include **requiring that exchanges perform technical due diligence to ensure the token satisfies reasonable security practices** and requiring that the exchange ensure that certain disclosures are made by the organizers of the project. We also suggest that the safe harbor require that the exchange have reached some reasonable conclusion that the token is not, in fact a security. This could be achieved, for example, by conditioning the application of the safe harbor on the receipt of an opinion from qualified counsel that the token does not qualify as a security under the Howey test. For example, **the safe harbor could apply only to tokens that relate to projects that are already operational or will be operational within a certain time period after listing.** The safe harbor could also include a condition requiring that listed

tokens include reasonable transfer restrictions on the founders and that the exchange take reasonable steps to limit the amount that any one individual token holder can purchase.” El resaltado es mío.

[730]

Confr. A. S. Myalo, *Comparative Analysis of ICO, DAOICO, IEO...o.c.* p. 10. Ampliar también en <https://hackernoon.com/overview-of-the-daico-crowdfunding-model-c611d55d4365>, recuperado el 30/04/2020.

[731]

Idem, p. 12.

[732]

Ibid.

[733]

Idem, p. 13. Ampliar también en Sergey Baloyan, *How to launch your IEO: Guide for projects + list of Exchanges*, recuperado el 27/04/2020 en <https://hackernoon.com/how-to-launch-your-ieo-guide-for-projects-list-of-exchanges-dcebca23bcac>, y en <https://medium.com/okex-blog/what-is-initial-exchange-offering-ieo-the-evolution-of-ieo-market-9c7492f06df8>, recuperado el 26/04/2020.

[734]

Ibid.

[735]

Confr. John Slyusarev, *Analytical report: IEOs in 2019-2020*, disponible al 28/04/2020 en <https://blog.coinmarketcap.com/2020/04/15/analytical-report-ieos-in-2019-2020/>.

[736]

Ibid.

[737]

Confr. IEO Guidelines, recuperado el 23/04/2020 en <http://www.koreaittimes.com/news/articleView.html?idxno=87177>.

[738]

Confr. <https://www.supercryptonews.com/south-korea-defi-risk-possible-ban-from-regulators/>, recuperado el 29/04/2020.

[739]

Se sigue en general la exposición ya expuesta en el artículo del autor: *Reflexiones sobre la tokenización de activos y su disruptivo potencial*, publicado en *Temas de Derecho Comercial, Empresarial y del Consumidor*, Ed. Errepar, Abril, 2020, cita digital: IUSDC3287330A

[740]

OECD (2020), *The tokenisation of Assets and Potential Implications for Financial Markets*, recuperado el 28/04/2020 de <https://www.oecd.org/finance/the-tokenisation-of-assets-and-potential-implications-for-financial-markets.htm>, p. 10.

[741]

Especial atención debe prestarse a los *atomic swaps*: la permuta *wallet-to-wallet* automatizada, i.e. embebida en un smart contract de tipo HTCL, entre dos activos digitales simultáneamente y en una misma operación, sin ningún tipo de

intermediario y sin comisiones (o con muy bajas comisiones).

[742]

Los oráculos permiten que las blockchains y los smart contracts que corren sobre ella puedan “acceder” a datos externos a la red, datos electrónicos del mundo real, datos éstos que pueden constituir condiciones o presupuestos que disparan determinadas acciones pre-programadas en un smart contract. Por tanto, los oráculos son servicios que verifican el acaecimiento (o no) de determinados hechos en el mundo real. Estos datos pueden provenir de software (big data) o de hardware (sensores de IoT o IIoT), que informan por ejemplo, temperatura, un pago exitoso, la fluctuación del precio de un commodity. Ampliar en <https://blockchainhub.net/blockchain-oracles/> recuperado al 29/04/2020.

[743]

Por ejemplo, un departamento de 100 metros cuadrados puede ser dividido en 100 tokens que se venden a inversores, y que representan 1 metro cuadrado cada uno, conteniendo el derecho a recibir el 1% del producido de la venta del inmueble, o de las rentas que genere el inmueble, si fuera alquilado. En lugar de vender un departamento a 100.000 U\$D a un inversor, el desarrollista emite un token que permite captar 100 inversores de 1.000 U\$S cada uno, con lo cual un proyecto inmobiliario de 50 unidades podría ser financiado por 5000 inversores de 1.000 U\$D cada uno, ampliando la base de inversores considerablemente y reduciendo 100 veces el tamaño del ticket de inversión.

[744]

Para una explicación profunda del funcionamiento de los Credit Default Swaps, véase del autor *Reflexiones sobre derivados sintéticos: la postura de la S.E.C. en el caso Goldman Sachs*, publicado en www.eldial.com, Supl. de Derecho Empresario, Junio de 2010.

[745]

Para que la entrega y el pago puedan ocurrir simultáneamente *on-chain*, se requiere alguna forma tokenizada de moneda *on-chain*. En la actualidad, las opciones son dos: (i) central bank tokenized cash, es decir, las CBDCs ya vistas, o (ii) *stablecoins*. Para profundizar en ambas alternativas, véase, del mismo autor, *Prueba de Impacto: Token Economics y Sustainable Finance*, en Diario La Ley, 09/12/2019.

[746]

OECD (2020), *The tokenisation..o.c.*, p. 32.

[747]

Este tercero de confianza no sería necesario en el caso de tokenización de activos nativos digitales.

[748]

Una interesante aplicación comienza a verse con los bonos verdes emitidos en blockchain. Véanse los interesantes casos analizados en la obra del autor, *Prueba de Impacto: Token Economics y Sustainable Finance*, en Diario La Ley, 09/12/2019, y en *Green Blocks: Impulsando la R/Evolución de los bonos verdes on-chain*, recuperado el 29/04/2020

en

<https://blockalizer.com/site/#/articulo;id=49iU9RIOwOpH3WWKPEnD2Q>.

[749]

Por ejemplo, la empresa suiza Mt. Pelerin, fue primera en tokenizar todas sus acciones emitidas y en circulación, emitiendo tokens en Ethereum (llamados MPS tokens). La firma igualmente mantiene un registro privado de accionistas, que no es reemplazado por la blockchain. Los tokens emitidos son libremente transferibles, pero el cesionario debe registrarse en el emisor antes de poder ejercer derechos políticos o económicos. Esta tokenización de acciones escriturales fue posible en el marco de la iniciativa de la Asociación Suiza de Mercado de Capitales y Tecnología, y en los hechos implica que una acción escritural no puede ser transferida sin transferir simultáneamente su token.

[750]

Por ejemplo, la firma inglesa Nivaura fue la primera en emitir un bono en Ethereum en el Reino Unido, registrando en una blockchain pública la emisión, la colocación, los pagos y automatizando procesos mediante smart contracts y acortado significativamente el período de tiempo involucrado de punta a punta del proceso. Todo el proceso, *end-to-end*, fue digitalizado en blockchain, y tanto la suscripción como los pagos a los inversores se hicieron en ETH. En ningún momento el bono tomó contacto con las infraestructuras financieras convencionales, y los fondos levantados (en ETHs) fueron transaccionados mediante smart contracts: en ningún momento Nivaura controló la alocaión de bienes y fondos. Los honorarios legales fueron reducidos, ya que la estructura y la documentación es más sencilla. Los pagos de servicios del bono se hacen peer-to-peer con smart contracts en ETHs, sin tener que contratar un agente de pago, o de custodia. Esta emisión fue enmarcada en en Sandbox de la Financial Conduct Authority inglesa.

[751]

Un ejemplo de estándar que regula smart contracts vinculados a valores negociables es el ERC1400. OECD (2020), *The tokenisation...*, p. 14.

[752]

Confr. <https://www.isda.org/2019/01/31/isda-and-linklaters-launch-full-version-of-isda-create-im/>, recuperado al 29/01/2020.

[753]

OECD (2020), *The tokenisation ...*, p. 15.

[754]

Confr. <http://ir.nasdaq.com/news-releases/news-release-details/nasdaq-link-enables-first-ever-private-securities-issuance> recuperado el 28/04/2020.

[755]

Confr. <https://www.sdx.com> recuperado la 28/04/2020.

[756]

Confr. <https://www.sesocio.com/articles/2019/07/18/la-criptomoneda-que-revoluciona-las-inversiones> recuperado el 28/04/2020.

[757]

Véase, del autor, *La plasticidad del fideicomiso financiero*, publicado en Foro de Córdoba N° 129, Agosto de 2008, p. 43, disponible en

<http://forodecordoba.com.ar/contenido.php?id=375>.

[758]

Experiencias ya generadas en securitizaciones relacionadas a, por ejemplo, (i) transparencia sobre colaterales (garantías de la emisión), (ii) las normas de protección del inversor, (iii) el derecho del tenedor del título sobre flujos de fondos subyacentes, (iv) los modos de articular esos derechos, (v) los deberes de conducta de los gestores de activos securitizados, y (vi) los pros & cons de los modelos de negocio de *originar y distribuir* (semilla de la crisis financiera de 2008/2011 que motivó, precisamente, el surgimiento de Bitcoin).

[759]

OECD (2020), *The tokenisation ...*, p. 51e.

[760]

Ibid.

[761]

Confr. <https://www.forbes.com/sites/rachelwolfson/2018/10/03/a-first-for-manhattan-30m-real-estate-property-tokenized-with-blockchain/#3273ba7e4895> recuperado el 30/04/2020.

[762]

Bajo un formato de crowdfunding inmobiliario apalancado en blockchain, el desarrollista del proyecto AnnA Villa emitió 10.000 tokens, con un valor mínimo de suscripción de 6.5€ cada uno, que representaban acciones de la sociedad (SPV) en cuyo activo se incorporó un edificio de lujo en París valuado en € 6.5 millones. Confr. <https://www.unlock-bc.com/news/2019-07-07/equisafe-completes-first-ever-blockchain-real-estate-sale-for-65-million> recuperado al 28/04/2020.

[763]

En efecto, la escalabilidad tecnológica de las DLTs, la interoperabilidad entre ellas, la **gran exposición** a riesgos cibernéticos, las alternativas de protocolo de gobierno (PoW vs. PoS vs. PoA, etc.), la ausencia de una única parte responsable por la red y su mantenimiento; la posibilidad de “ataques del 51%”; la computación cuántica vs. la encriptación asimétrica, etc.

[764]

Especialmente en materia de privacidad, protección de datos, almacenamiento de datos y su monetización; el “derecho al olvido”; identidad digital; anonimidad y pseudonimidad vs. el cumplimiento de normas de KYC/AML.

[765]

Un resumen del mismo puede encontrarse aquí <https://www.allenoverly.com/en-gb/global/news-and-insights/publications/uk-jurisdiction-taskforce-the-lawtech-delivery-panel-legal-statement-on-cryptoassets>, disponible al 30/04/2020.

[766]

OECD (2020), *The tokenisation ...*, p. 21.

[767]

OECD (2020), *The tokenisation ...*, p. 29.

[768]

Ibid.

[769] Confr. <http://www.bcra.gov.ar/Noticias/Mesa-innovacion-financiera.asp>, recuperado el 28/04/2020.

[770] Confr. <https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1332/1332grupo-de-trabajo-fintech> recuperado al 28/04/2020.

[771] Confr. A. S. Myalo y N. Yu Glukov, *Factors of success of Initial ...o.c.*, p. 36.

[772] Ibid.

[773] Confr. Roger Brownsword, *Regulatory fitness: Fintech, Funny Money and Smart Contracts*, publicado en *European Business Organization Law Review*, 2019, número 20, p. 11. Ejemplifica Brownsword a los “coherentes” en estos términos: “*When they are called on to respond to new technological developments, **coherentists tend to try to classify the new phenomena within existing legal categories.** For example, a nice coherentist question might be whether, with humans out of the transactional loop, **automated and autonomous performance systems could be treated relative to recognised legal concepts and categories (such as the limited liability company) as having their own legal personality.** Similarly, when the technologies that support e-commerce appeared, the coherentist response was to try to fit the legal template for off-line contracts to the emerging world of on-line transactions.*”. Ejemplifica el enfoque de regulación instrumental en este modo: “*Unlike a coherentist conversation, a regulatory-instrumentalist conversation will not focus on the application of the law of contract to smart contracts. Rather, the conversation will seek to **identify the potential benefits and risks of committing transactions (or parts of transactions) to a blockchain and it will then strive to find an acceptable balance between management of the risks and not stifling enterprise.** The challenge is to find the regulatory sweet spot, **neither over-regulating (and stifling innovation) nor under-regulating and exposing parties to unacceptable risks.**”*

[774] Confr. FCA, *Discussion paper on distributed ledger technology*, recuperado el 26/04/2020 en <https://fca.org.uk/publication/discussion/dp17-03.pdf>, puntos 1.4 y 1.17.

[775] Véase el informe del Government Office for Science, *FinTech Futures – the UK as a World leader in Financial Technologies*, 2015, disponible el 26/04/2020 en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415331/15-3-fintech-futures.pdf.

[776] Idem, puntos 1.7-1.9.

[777] Ampliar en <https://www.fca.org.uk/firms/innovation/direct-support>, recuperado el 27/04/2020.

[778] Confr. FCA, *The impact and effectiveness of Innovate*, recuperado el 26/04/2020 en <https://www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf>.

[779] Ampliar en <https://www.fca.org.uk/firms/innovation/advice-unit>, recuperado el 27/04/2020.

[780] Ampliar en <https://www.fca.org.uk/firms/innovation/regulatory-sandbox>, disponible al 26/04/2020.

[781] Confr. FCA, *The impact and effectiveness...o.c.* p. 5.

[782] Ampliar en <https://www.fca.org.uk/firms/innovate-and-innovation-hub/engagement>, recuperado el 22/04/2020.

[783] Ampliar en <https://www.fca.org.uk/firms/innovation/global-financial-innovation-network>, recuperado el 23/04/2020.

[784] Ampliar en <https://static1.squarespace.com/static/5db7cdf53d173c0e010e8f68/t/5dbfaaca6b4e151d/One-year-on-FINAL-20190612+%28CLEAN+VERSION%29.pdf>, recuperado el 28/04/2020.

[785] Confr. Renato Mangano, *Blockchain securities, insolvency law and the Sandbox approach*, publicado en *European Business Organization Law Review*, 2018, número 19, p. 728.

[786] Confr. FCA, *The impact and effectiveness of Innovate...p. 18*, donde se señala: “of the 44 start-ups that tested in cohorts 1,2 and 3 of the Sandbox, 17 were either acquired or received investment during or after their test. 15 start-ups participated in cohort 1, and of these 2 have been acquired, and 6 have gone on to receive a combined total of over £135m of equity funding. We see similar stats through our Direct Support function, where 13 out of the first 50 firms we supported received subsequent investment to a value of over £165m.”

[787] Confr. Deloitte, *A journey through the FCA regulatory sandbox*, recuperado el 27/04/2020 en <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-fca-regulatory-sandbox-project-innovate-finance-journey.pdf>, p. 2.

[788] Disponibles, al 27/04/2020 en <https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application>.

[789] Confr. Deloitte, *A journey through the FCA regulatory...o.c.*, p. 3.

[790] Confr. Renato Mangano, *Blockchain securities...* p. 729.

[791] Confr. FCA, *The impact and effectiveness of Innovate...*p. 22.

[792] Véase <https://www.fca.org.uk/firms/regulatory-sandbox/cohort-5>, disponible al 25/04/2020.

[793] Confr. Renato Mangano, *Blockchain securities...* p. 732. Señala Mangano que se produce una negociación del tipo win-win entre el regulador y el regulado: “*Even though the FCA has not formalized the context for this bargaining, this activity appears to follow an ideal framework where the FCA and the firms admitted to the sandbox pursue their respective goals under the pressure of their respective incentives. These incentives are: for the FCA, the concern that the **firms offering digital securities might decide to quit the UK market for a more permissive market**; and, for the firms admitted to the sand-box, their interest in **obtaining an authorization in one of the largest financial markets around the world** or, if this authorization is considered as unnecessary for them, their interest in being formally accredited in the UK financial market. Further, the FCA has set the rules of the ‘game’, for example by establishing that the sandbox operates on a cohort basis and that the admitted firms might be requested to adjust their products; finally, the FCA makes the results of this activity public.*” El resultado es mío.

[794] Confr. Karen Yeung, en *Regulation by blockchain..* p. 233.

[795] Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 541.

[796] Ibid.

[797] Ibid.

[798] El Consejo de Ministros aprobó un anteproyecto de Ley que implementará un SandBox. Confr. <https://es.cointelegraph.com/news/spain-approves-a-bill-to-create-a-sandbox-for-fintech>, recuperado el 28/04/2020.

[799] Confr. BID, *SandBox regulatorio en América Latina y el Caribe para el Ecosistema Fintech y el sistema financiero*, disponible el 28/04/2020 en <https://publications.iadb.org/publications/spanish/document/Sandbox-regulatorio-en-América-Latina--el-Caribe-para-el-ecosistema-Fintech-y-el-sistema-financiero.pdf>.

[800] Confr. <https://asic.gov.au/for-business/innovation-hub/fintech-regulatory-sandbox/>, disponible al 27/04/2020.

[801] Confr. Comisión Europea, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS –FinTech Action plan: For a more competitive and innovative European financial sector*, disponible al 27/04/2020 en https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf, p. 9.

[802]

Confr. <https://nssc.novascotia.ca/sites/default/files/docs/Feb.%2023,%202017%20CSA%20Regpress%20release-Final.pdf>, recuperado el 27/04/2020.

[803]

Confr. FCA, *Guidance on Cryptoassets*, recuperado el 22/04/2020 en <https://www.fca.org.uk/publication/policy/ps19-22.pdf>.

[804]

Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 4, sostiene que “*These are not issued or backed by any central authority and are intended and designed to be used as a means of exchange. They tend to be a decentralised tool for buying and selling goods and services without traditional intermediaries. These tokens are usually outside the perimeter.*”

[805]

Ibid. Se afirma que “*these tokens grant holders access to a current or prospective product or service but do not grant holders rights that are the same as those granted by specified investments. Although utility tokens are not specified investments, they might meet the definition of e-money in some circumstances (as could other tokens). In this case, activities involving them may be regulated. Utility tokens provide consumers with access to a current or prospective service or product and often grant rights similar to pre-payment vouchers. In some instances, they might have similarities with, or be the same as, rewards-based crowdfunding. Here, participants contribute funds to a project in exchange, usually, for some reward, for example access to products or services at a discount. Much like exchange tokens, utility tokens can usually be traded on the secondary markets and be used for speculative investment purposes. This does not in itself mean these tokens constitute specified investments if they do not have the characteristics of relevant specified investments.*” El resaltado es mío.

[806]

Ibid. Se afirma que “*These are tokens with specific characteristics that mean they provide rights and obligations akin to specified investments, like a share or a debt instrument. These tokens are within the perimeter.*” El resaltado es mío.

[807]

Texto disponible aquí: <http://www.legislation.gov.uk/ukxi/2001/544/contents/made>. Según el tipo de security token de que se trate, también pueden ser aplicables las normas sobre Dinero Electrónico, sobre Servicios de Pago, y la Directiva Europea sobre Mercados de

Instrumentos Financieros (MiFID). Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 4, punto 1.10.

[808] Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 45, punto 69, aclara: “E-money is electronically stored monetary value as represented by a claim on the electronic money issuer which is: issued on receipt of funds for the purpose of making payment transactions, **accepted by a person other than the electronic money issuer and not excluded by regulation 3 of the EMRs. E-money must enable users to make payment transactions with third parties, so must be accepted by more parties than just the issuer. E-money includes fiat balances in various types of online wallets or prepaid cards.**” El resaltado es mío.

[809] Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 13, punto 2.25 indica que se creará una nueva categoría de e-money token, que es distinta a la de un utility token puro, que no está ni estará regulado, y se aclara que “These tokens can, for example, be issued centrally or be decentralised, give access to a current or prospective good or service in one or multiple networks and ecosystems, or be used as a means of exchange. They can be fully transferable or have restricted transferability. **These tokens fall outside the regulatory perimeter.**”

Con relación a las monedas estables, se aclara que “not all tokens where attempts have been made to stabilise their value will be e-money. Tokens must also meet the other criteria in the definition of e-money set out in the EMRs. For example, a token that is backed with fiat currency, **but can only be spent with the issuer will not constitute e-money**, as it is not accepted by a person other than the issuer (...)

While these tokens may not meet the definition of e-money, they could fall inside the perimeter in other ways, for example, as security tokens. **Depending on structure and arrangement, tokens could meet the definition of units in a collective investment scheme, debt securities or other types of specified investments.** Given the structure of rights attached to such tokens varies greatly, judgements on whether they fall under the scope of regulation can only be made on a case-by-case basis. Tokens that do not meet the definition of an e-money token, or the definition of a security token, will be unregulated tokens...**Any token that is not a security token, or an e-money token is unregulated.** For instance, a ‘stablecoin’ could be considered a unit in a collective investment scheme, a debt security, e-money or another type of specified investment. It might also fall outside of the FCA’s remit. Ultimately, this can only be determined on a case-by-case basis.” El resaltado es mío.

[810] Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 33, punto 30 aclara los criterios que la FCA analiza para determinar si el token es un security: “Given the complexity of many tokens, it is not always easy to determine whether a token is a specified investment, specifically those types of specified investment that are securities, like shares or debt instruments. There are a few factors that are indicative of a security. These factors may

include, but are not limited to: i) the contractual rights and obligations the token-holder has by virtue of holding or owning that cryptoasset, ii) any contractual entitlement to profit-share (like dividends), revenues, or other payment or benefit of any kind, iii) any contractual entitlement to ownership in, or control of, the token issuer or other relevant person (like voting rights), iv) the language used in relevant documentation, like token 'whitepapers', that suggests the tokens are intended to function as an investment, **although it should be noted that the substance of the token (and not the label used) will determine whether an instrument is a specified investment** – For example, if a whitepaper declares a token to be a utility token, but the contractual rights that it confers would make it a share or a unit in a collective investment scheme, we would consider it to be a security token, v) If the flow of payment were a contractual entitlement we would consider this to be a strong indication that the token is a security, irrespective of whether the flow of payment is direct or indirect (or whether other ownership rights are present).” Los resultados son míos.

[811] Confr. FCA, *Guidance on Cryptoassets..o.c.*, p. 21, punto 4.6.

[812] Ibid.

[813] Véase <https://technation.io/about-us/>. La asociación cuenta con más de 600 empresas asociadas, y el 80% de sus costos operativos son solventados por el Department for Digital, Culture, Media & Sports del Gobierno del Reino Unido.

[814] Confr. <https://technation.io/about-us/lawtech-panel/>, recuperado el 28/04/2020.

[815] Confr. UKJT, *Legal statement on cryptoassets and smart contracts*, recuperado el 28/04/2020 en https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111.1.pdf.

[816] Confr. UKJT, *Legal statement on cryptoassets...*p. 3.

[817] Confr. UKJT, *Legal statement on cryptoassets...*p. 10.

[818] Idem, p. 13.

[819] Ibid.

[820] Ibid.

[821] Idem, p. 14.

[822] Idem, p. 17. Se afirma que: “*the commercial value of a cryptoasset is not in the recorded data itself but in the fact that the person possessing that data is able to effect and authenticate dealings in the cryptoasset in accordance with the rules of the*

system. Putting it another way, it is not what the data tells you but what it allows you to do” y que “Cryptoassets can in that respect be contrasted with other digital assets, such as databases or digital photographs or computer programmes, the value of which is in the very information that they contain or comprise. Cryptoassets can also be contrasted with trade secrets, business ideas, private communications or personal information, where, again, it is the information itself, and what it conveys, that is of interest and value. **A cryptoasset does not convey anything, it is instead merely a token to be used within the system.**” (El resaltado es mío).

[823]

Confr. UKJT, *Legal statement on cryptoassets...*p. 7.

[824]

Ibid.

[825]

Idem, p. 25. Afirman que: “English law only recognises four kinds of consensual security: pledge, contractual lien, equitable charge and mortgage. Pledges and liens can only be created if it is possible to transfer possession of an asset. Since cryptoassets cannot be possessed, they cannot be the object of a pledge or lien. If a particular cryptoasset is property, **a mortgage or equitable charge can be created over it.** This can be done in the same way that a mortgage or equitable charge can be created over other intangible property, and subject to the same requirements.” El resaltado es mío.

[826]

Idem, p. 26.

[827]

Idem, p. 31.

[828]

Ibid.

[829]

Ibid. Tales requisitos son: “The requirements for formation of a contract are three-fold: first, that agreement has, objectively, been reached between the parties as to terms that are sufficiently certain; secondly, that the parties intended (again, objectively) that they would be legally bound by their agreement; thirdly that, unless the contract is made by deed, each party to it must give something of benefit, which is referred to as “consideration”—a gratuitous promise in return for nothing is not generally enforceable.... In a commercial context, agreement is generally found in, or at least evidenced by, a written document bearing signatures of the parties—but **neither writing nor signature is a necessary precondition for a contract to be identified or for it to have force.**” El resaltado es mío.

[830]

Ampliar en <https://medium.com/@hackersleaguebooks/what-is-source-code-and-object-code-4a010304da2b>, recuperado el 26/04/2020.

[831]

Idem, p. 38.

[832]

Idem, p. 36.

[833] Idem, p. 37.

[834] Confr. Uniform Law Commission, *Regulation of Virtual-Currency Businesses Act*, recuperado el 28/04/2020 en <https://www.uniformlaws.org/committees/community-home?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778>.

[835] Confr. Ley Modelo, nota explicatoria, disponible al 28/04/2020 en <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=ef45a10b-ac62-ad3d-2f42-588d7eac3e40&forceDialog=0>, p. 4: “*Virtual currency, as defined in § 102(23), (A) means a digital representation of value that: (1) is used as a medium of exchange, unit of account, or store of value; and (2) is not legal tender, whether or not denominated in legal tender; and (B) does not include: (1) a transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank credit, or virtual currency; or (2) a digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.*”

[836] Idem, p. 5, define a los *Exchange* como: “*Section 102(5) defines the term “exchange” as ...to assume control of virtual currency from or on behalf of a resident, at least momentarily, to sell, trade or convert: (A) virtual currency for legal tender, bank credit, or for one or more forms of virtual currency; or (B) legal tender or bank credit for one or more forms of virtual currency.*”

[837] Confr., Ley Modelo, nota explicatoria, disponible al 28/04/2020 en <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=ef45a10b-ac62-ad3d-2f42-588d7eac3e40&forceDialog=0>.

[838] Confr. <https://coincenter.org/link/the-ulc-s-model-virtual-currency-regulation-has-been-introduced-in-hawaii-nebraska>, recuperado el 28/04/2020.

[839] Confr. https://www.capitol.hawaii.gov/Archives/measure_indiv_Archives.aspx?billtype=SB&billnumber=2129&year=2018 recuperado el 29/04/2020.

[840] Texto de la ley disponible al 23/04/2020 en <https://www.flsenate.gov/Session/Bill/2017/1379/BillText/er/PDF>.

[841] Confr. <https://www.natlawreview.com/article/florida-creates-blockchain-task-force-to-study-benefits-blockchain-technology>, recuperado el 29/04/2020.

[842] Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 377.

[843] Ibid. Es el caso de Nueva York y Arizona.

[844] El texto de la ley está disponible, al 27/04/2020 en <https://www.congress.gov/bill/115th-congress/house-bill/6913/text>.

[845] Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 381.

[846] Confr. Mike Orcutt, *States that are passing laws to govern “smart contracts” have no idea what they’re doing*, publicado en MIT Technology Review, recuperado el 28/04/2020 en <https://www.technologyreview.com/2018/03/29/144200/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/>.

[847] Véase CDC, *Joint Statement in response to State “Smart Contracts” legislation*, disponible al 28/04/2020 en <https://digitalchamber.org/wp-content/uploads/2018/07/Smart-Contracts-letter-cover.png>.

Véase también: Amy Davine Kim y Perianne Boring, *State-by-state smart contract laws? If it ain’t broke, don’t fix it*, recuperado el 28/04/2020 de <https://www.coindesk.com/state-state-smart-contract-laws-aint-broke-dont-fix>.

Afirman que: “*the federal Electronic Signatures in Global and National Commerce Act (ESIGN Act) and the Uniform Electronic Transactions Act (UETA) provide an unquestionable legal basis for smart contract technology executing the terms of a legal contract. Once cryptographically signed, legal efficacy is granted to electronic signatures, records, and contracts so long as the parties are provided with appropriate written notice and consent to conduct business electronically*” y sostienen que “*Cryptographic signatures (also known as digital signatures), records, or contracts used to execute the terms of a legal contract, entirely or in part, fall squarely within the ambit of the UETA and ESIGN Act. In fact, the ESIGN and UETA legislation were designed to avoid state-by-state enactment of individual laws recognizing digital signatures and records. Any additional regulation would be, at best, redundant. The Chamber of Digital Commerce has investigated the legal underpinnings of these laws and concluded that enactment of state legislation regarding smart contracts is unnecessary and potentially undermines the growth of the industry.*” El resaltado es mío.

[848] Confr. <https://legiscan.com/AZ/text/HB2417/id/1588180>, recuperado el 01/05/2020. Definió a los contratos inteligentes como: “*AN EVENT-DRIVEN PROGRAM, WITH STATE, THAT RUNS ON A DISTRIBUTED, DECENTRALIZED, SHARED AND REPLICATED LEDGER AND THAT CAN TAKE CUSTODY OVER AND INSTRUCT TRANSFER OF ASSETS ON THAT LEDGER.*”

[849]

La ley define a la blockchain como: “*DISTRIBUTED LEDGER TECHNOLOGY THAT USES A DISTRIBUTED, DECENTRALIZED, SHARED AND REPLICATED LEDGER, WHICH MAY BE PUBLIC OR PRIVATE, PERMISSIONED OR PERMISSIONLESS, OR DRIVEN BY TOKENIZED CRYPTO ECONOMICS OR TOKENLESS. THE DATA ON THE LEDGER IS PROTECTED WITH CRYPTOGRAPHY, IS IMMUTABLE AND AUDITABLE AND PROVIDES AN UNCENSORED TRUTH.*”

[850]

Confr. Jeffrey Neuburger, *Arizona passes groundbreaking blockchain and smart contract law – State blockchain laws on the rise*, recuperado el 29/04/2020 en <https://newmedialaw.proskauer.com/2017/04/20/arizona-passes-groundbreaking-blockchain-and-smart-contract-law-state-blockchain-laws-on-the-rise/>.

[851]

Confr. Jared Arcari, en *Decoding Smart Contracts...o.c.*, p. 388.

[852]

Ampliar en Colin Wood, *Nevada lawmakers approve four blockchain bills*, recuperado el 28/04/2020 en <https://statescoop.com/nevada-lawmakers-approve-four-blockchain-bills/>.

[853]

Confr. <https://esignrecords.org/2017/06/09/nevada-law-adds-blockchain-smart-contract-recognition-state-statutes/>, recuperado el 29/04/2020.

[854]

Texto de la ley disponible al 29/04/2020 en <https://legiscan.com/NV/bill/SB161/2019>.

[855]

Texto de la ley disponible al 29/04/2020 en <https://legiscan.com/NV/bill/SB162/2019>.

[856]

Texto de la ley disponible al 29/04/2020 en <https://legiscan.com/NV/bill/SB163/2019>.

[857]

Confr. <http://www.capitol.tn.gov/Bills/110/Bill/HB1507.PDF>, recuperado el 22/04/2020.

[858]

Al 24/04/2020 el texto de la ley está disponible aquí: <https://www.nysenate.gov/legislation/bills/2019/s4142>.

[859]

Ampliar en <https://statescoop.com/bitlicense-roundtable-convenes-in-new-york-as-senators-consider-overhaul/> disponible al 25/04/2020.

[860]

Confr. Daniel Roberts, *Behind the “exodus” of bitcoin startups from New York*, en <https://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>, disponible al 28/04/2020. Afirma Roberts que la regulación estadual produjo un éxodo masivo de *Exchanges*, ya que “*requires a licensed company to submit to a biennial*

examination of financial records, management policies and general compliance, while also granting the superintendent of Financial Services the ability to regulate mergers and changes of control in virtual currency transmission companies. Further complicating matters, an anti-money laundering program and a cybersecurity program are also required to obtain a BitLicense.” Se requiere una BitLicense para realizar cualquiera de estas actividades: “*Virtual currency transmission; Storing, holding, or maintaining custody or control of virtual currency on behalf of others; Buying and selling virtual currency as a customer business; Performing exchange services as a customer business, and Controlling, administering, or issuing a virtual currency”*. Confr. https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_fa En Diciembre de 2019 se analizaban cambios en el BitLicense, habiéndose hecho públicas las directrices de la nueva regulación y solicitando comentarios de partes interesadas hasta el 20 de Enero de 2020: https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/pr_guidance disponible al 28/04/2020. Hasta Abril de 2020 se han concedido solo 18 BitLicenses.

[861] Puede ampliarse en <https://www.coindesk.com/4-blockchain-bills-introduced-new-york-legislature>, disponible al 24/04/2020.

[862] Específicamente en relación a la validez de los contratos inteligentes, la ley de Nueva York reza: “*The state technology law is amended by adding a new section 310 to read as follows:§ 310. Signatures and records secured through blockchain technology and smart contracts. 1. A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature. 2. A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record. 3. **Smart contracts may exist in commerce.** A contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term. 4. Notwithstanding any other law, rule or regulation to the contrary, a person that, in or affecting interstate or foreign commerce, uses blockchain technology to secure information that the person owns or has the right to use retains the same rights of ownership or use with respect to that information as before the person secured the information using blockchain technology. This subdivision does not apply to the use of blockchain technology to secure information in connection with a transaction to the extent that the terms of the transaction expressly provide for the transfer of rights of ownership or use with respect to that information.”* (El resaltado es mío).

[863] Al 24/04/2020 el texto de la ley está disponible aquí: https://assembly.state.ny.us/leg/?default_fld=&bn=A08792&term=2017&Summary=Y&Actions=Y&Text=Y&Committee

[864]

Confr. <https://legislature.vermont.gov/statutes/section/12/081/01913>, recuperado el 01/05/2020. La ley reconoce carácter probatorio *iuris tantum* a los registros extraídos de una blockchain en estos términos: “(3) *The following presumptions apply: (A) A fact or record verified through a valid application of blockchain technology is authentic. (B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain. (C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation. (D) If the parties before a court or other tribunal have agreed to a particular format or means of verification of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record.*”

[865]

Al 24/04/2020 el texto de la ley está disponible aquí: <https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT205/ACT205%20A>

[866]

Confr. <https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html> recuperado el 22/04/2020.

[867]

Confr. <https://illinoisblockchain.tech>, recuperado el 28/04/2020.

[868]

Confr. <https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html> recuperado el 22/04/2020.

[869]

El texto de las reformas se encuentra, al 26/04/2020 en <https://legis.delaware.gov/BillDetail?legislationId=25730>. Véase también David Lucking, *Delaware passes law permitting companies to use blockchain technology to issue and track shares*, disponible en la misma fecha. Señala Lucking que las “*blockchain shares will be legally considered as a form of **uncertificated securities**. In the amendment to Section 219, the term “stock ledger” is to be defined to include ledgers “administered by or on behalf of the corporation,” to permit a record keeping system utilizing blockchain databases. Within Section 224, a change has been made to permit all corporate records to be kept on “one or more electronic networks or databases (including one or more distributed electronic networks or databases)”. In order to satisfy legislative requirements, the ledger must: (i) allow the production of a record of the company’s stockholders; (ii) record certain mandatory information; and (iii) permit transfer of stock. There is also a requirement within Section 224 that **any record held on an electronic network or database must be capable of being converted into ‘clearly legible paper form’**, upon the request of a person entitled to inspect the records. Section 224 goes on to clarify that such paper record derived from the electronic network or database **would be valid and admissible in evidence and accepted for all other***

purposes that an original paper record would be. A further clarification was made in Section 232, confirming that **"the use of, or participation in, one or more electronic networks or databases (including one or more distributed electronic networks or databases)" is considered within the existing definition of 'electronic transmission'**. Alongside the general benefits of efficiency and security, **smart contract technology could also be used to code any requirements or preferred options into the digital shares themselves so that covenants are automatically complied with**. Voting and other corporate actions could be simplified and audits streamlined. Regulators could also have real-time access and transparency."El resaltado es mío.

[870]

Confr. Andy Singleton, *A first: Delaware stock on the blockchain*, recuperado el 28/04/2020 en <https://medium.com/aboveboard-news/stock-on-the-blockchain-is-here-dc7421dbecd1>. Véase también la reputada opinión de la directora de DBI, Andrea Tinianow, *Tokenized securities are not secured by Delaware Blockchain Amendments*, disponible al 28/04/2020 en <https://www.forbes.com/sites/andreatinianow/2018/07/04/tokenized-securities-are-not-secured-by-delaware-blockchain-amendments/#21ba88553e79>, quien afirmaba que *"a Delaware corporation may issue shares and maintain its stock ledger on a blockchain (through smart contract functionality), without the need for a single central officer or agent (e.g., the corporate secretary or transfer agent) to serve as the recorder and clearing house for all issuances and transfers. Indeed, the Delaware Blockchain Amendments eliminated the requirement that any such officer or agent be responsible for updating the corporation's records, including its stock ledger, providing instead that the stock ledger constitutes one or more records "administered by or on behalf of the corporation" and that records administered by or on behalf of the corporation, including the stock ledger, may be kept on or by means of one or more electronic networks, including one or more distributed electronic networks or databases."*

[871]

Ibid. Se señalan las siguientes características de las primeras tokenized stocks: "i) *Compliance without a subscription agreement. The token itself is programmed with the rules for handling private stock. In the United States, the relevant rules are regulation D and S*, ii) *Global distribution. Investors from many different countries can acquire the stock after qualifying to be on local blockchain "whitelists". One security and one registry can use information from many different whitelists*, iii) *Liquidity. Approved investor categories can trade this security on the emerging exchanges for private and public tokenized securities*, iv) *Control of transfers. The issuer can turn trading off, globally, with a switch in the registry, and turn it on after "disclosing" all relevant information*, v) *Control of ownership. The issuer can also add and remove approved owners and investor categories*, vi) *Replacement of lost or hacked shares. Unlike cryptocurrencies, programmable securities are safe for investors that care about custody*, vii) *Real time visibility into the list of shareholders*; viii) *Membership and utility. The stock will be*

required a “stake” for brokers participating in our distributions.”

[872]

Confr. Andrea Tinianow y Caitlin Long, *Delaware Blockchain Initiative: transforming the Foundational Infrastructure of Corporate Finance*, publicado en Harvard Law School Forum on Corporate Governance, disponible al 26/04/2020 en <https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/>.

[873]

El texto de la ley puede encontrarse, al 28/04/2020 en <http://www.ilga.gov/legislation/publicacts/101/101-0514.htm>.

[874]

Confr. <https://www.natlawreview.com/article/illinois-embraces-smart-contracts-new-blockchain-legislation>, disponible el 28/04/2020. La ley admite cuatro usos para la blockchain y los contratos inteligentes: “(1) *A smart contract, record, or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.*

(2) *In a proceeding, evidence of a smart contract, record, or signature must not be excluded solely because a blockchain was used to create, store, or verify the smart contract, record, or signature.*

(3) *If a law requires a record to be in writing, submission of a blockchain which electronically contains the record satisfies the law.* (4) *If a law requires a signature, submission of a blockchain which electronically contains the signature or verifies the intent of a person to provide the signature satisfies the law.”*

[875]

Ibid. También se indican casos en los que los contratos inteligentes pueden no tener validez legal: (1) *If any law requires a contract to be in writing to be enforceable, a smart contract may be denied enforceability unless it is capable of being retained and accurately reproduced later by all parties.* This provision may address personal service contracts or agreements subject to a statute of frauds, which may require that the agreement be in writing to be enforceable. (2) *If any other law requires a record to be posted or sent in a specific manner, the record must still comply with that law to be enforceable.*(3) *If a person inhibits the ability of another person to store or retrieve information contained in a blockchain, such information is not enforceable by the person who inhibited the storage or retrieval.* This provision may assist parties to smart contracts that were not privy to drafting of the smart contract code. (4) *Notice or confirmation of receipt of notice may not be sent over blockchain in certain situations of public policy, such as cancelling a public utility, notice of default or eviction, cancellation of health benefits, or recall of products.* (5) *A writing requirement is not satisfied by use of a blockchain in cases regarding the transportation of hazardous materials.* (6) *The requirements of the BTA may not be altered by agreement, except when another law imposes certain writing requirements or first-class mailing requirements but permits parties to vary those requirements by agreement.”* (el resaltado

es mío).

[876] Puede ampliarse en <https://publications.tnsosfiles.com/acts/110/pub/pc0591.pdf>, disponible al 28/04/2020.

[877] Puede ampliarse en Caitlin Long, *What do Wyoming's 13 new blockchain laws mean?* Disponible al 13/05/2020 en <https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#3bb5d78a5fde> y en Michele Kulerman y Rebecca DiStefano, *Recent Rocky Mountain state law blockchain developments*, recuperado el 29/04/2020 en <https://www.natlawreview.com/article/recent-rocky-mountain-state-law-blockchain-developments>.

[878] Confr. <https://wyoleg.gov/2019/Summaries/SF0125.pdf>, disponible al 18/04/2020. Se indica que: “*This act establishes the legal nature of digital assets within existing law, dividing these assets into **three categories of intangible personal property** and classifying these assets within the Uniform Commercial Code (UCC) as follows:i) Digital consumer assets (UCC: general intangibles);ii) Digital securities (UCC: securities and investment property); and iii) Virtual currency (UCC:money).*” Caitlin Long, *What do Wyoming's 13 new blockchain laws mean...*o.c. afirma que Wyoming fue el primer Estado en eximir a los utility tokens de toda la legislación estadual sobre títulos valores con oferta pública.

[879] Texto disponible al 28/04/2020 en <https://wyoleg.gov/Legislation/2019/SF0125>. Se define al Smart Contract como “*an automated transaction, as defined in W.S. 40-21-102(a)(ii), or any substantially similar analogue, which is comprised of code, script or programming language that executes the terms of an agreement, and which may include taking custody of and transferring an asset, or issuing executable instructions for these actions, based on the occurrence or nonoccurrence of specified conditions.*”

Se definen también los acuerdos de firma conjunta: “*Multi-signature arrangement*” means a system of access control relating to a digital asset for the purposes of preventing unauthorized transactions relating to the asset, in which two (2) or more private keys are required to conduct a transaction, or any substantially similar analogue.” Y se define también a la llave privada en estos términos: “*a unique element of cryptographic data, or any substantially similar analogue, which is:(A) Held by a person; (B) Paired with a unique, publicly available element of cryptographic data; and (C) Associated with an algorithm that is necessary to carry out an encryption or decryption required to execute a transaction.*”

[880] Confr. Caitlin Long, *What do Wyoming's 13 new blockchain laws mean?*..o.c. El texto de esta ley está disponible al 13/05/2020 en <https://www.wyoleg.gov/Legislation/2019/hb0074>

[881] El texto de la ley está disponible al 13/05/2020 en <https://www.wyoleg.gov/Legislation/2019/hb0113>

[882] Confr. Caitlin Long, *What do Wyoming's 13 new blockchain laws mean?..o.c.*

[883] Véase el proyecto de ley en tratamiento actualmente en el estado de California disponible al 29/04/2020 en: Al 29/04/2020 el texto de la ley está disponible aquí: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1489.

[884] Confr. Andrea Tinianow, *A Split emerges in blockchain law: Wyoming's approach versus the supplemental act*, recuperado el 26/04/2020 en <https://www.forbes.com/sites/andreatinianow/2019/03/07/a-split-emerges-in-blockchain-law-wyomings-approach-versus-the-supplemental-act/#5242d730719a>.

Caitlin Long, *What do Wyoming's...o.c.* afirma que Wyoming ha autorizado “*the first true “qualified custodian” for digital assets which is a bank. Wyoming banks can start such operations as soon as September 1, 2019. Wyoming’s digital asset custodians will stand out above all others because they will respect the DIRECT ownership nature of digital assets! These new custodians won't be like traditional securities custodians, because for a Wyoming-based custodian investors will still DIRECTLY own their digital assets under custody as a BAILMENT, which means they retain direct ownership while merely giving up control (much like valet parking). Today, institutional investors are forced to be de facto creditors of their securities custodians, since all publicly-traded securities are owned indirectly. Custody under bailment is possible in securities custody today, but it's neutered by the fact that all securities are owned indirectly—investors can't directly own the real security, and therefore they're really just counterparties to the custodian. So, what Wyoming has done is truly revolutionary—BAILMENT + DIRECT ownership! It doesn't exist in securities custody today! Customers of Wyoming custodians can still choose indirect ownership, but it's on much more investor-friendly terms than exist in securities custody today. In sum, Wyoming will become known as the home of SOLVENT, investor-friendly digital asset custodians to which investment fiduciaries are likely to migrate over time.*” Los resaltados son míos.

[885] El texto de esta ley modelo está disponible al 28/04/2020 en <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=de52d1fe-1f70-a568-9552-d354ade157ca&forceDialog=0>.

[886] Confr. Andrea Tinianow, *A Split emerges in blockchain law: Wyoming's ...o.c.*

[887] Ibid.

[888] Al 29/04/2020 el texto de la ley está disponible aquí:

https://coloradosun.com/wp-content/uploads/sites/15/2019/01/19-0314_01.pdf.

[889] Puede ampliarse en Tamara Chuang, *Another push for Colorado blockchain law has more than token support*, recuperado el 29/04/2020 en <https://coloradosun.com/2019/01/04/another-push-for-colorado-blockchain-law-has-more-than-token-support/>.

[890] Al 29/04/2020 el texto de la ley está disponible aquí: https://leg.colorado.gov/sites/default/files/documents/2019A/bills/2019a_1247_01.pdf.

[891] Confr. Michele Kulerman y Rebecca DiStefano, *Recent Rocky Mountain state law blockchain developments..o.c.*

[892] Confr. <https://www.coinspeaker.com/us-cryptocurrency-act-2020-congressman/>, recuperado el 20/04/2020.

[893] El texto de la ley, al 28/04/2020 está disponible en: <https://s3.cointelegraph.com/storage/uploads/view/a7b9c3d6c50453c5580820ef0b09f5>.

[894] Ibid. “The term “crypto-commodity” means economic goods or services, including derivatives, that— (A) have full or substantial fungibility; (B) the markets treat with no regard as to who produced the goods or services; and (C) rest on a blockchain or decentralized cryptographic ledger.”

[895] Ibid. “The term “crypto-currency” means representations of United States currency or synthetic derivatives resting on a blockchain or decentralized cryptographic ledger, including— (A) such representations or synthetic derivatives that are reserve-backed digital assets that are fully collateralized in a correspondent banking account, such as stablecoins; and (B) synthetic derivatives that are—(i) determined by decentralized oracles or smart contracts; and (ii) collateralized by crypto-commodities, other crypto-currencies, or crypto-securities.”

[896] Ibid. “The term “crypto-security” means all debt and equity that rest on a blockchain or decentralized cryptographic ledger. The term “crypto-security” does not include a synthetic derivative that— (i) is operated as, and is registered with the Department of the Treasury as, a money services business; and (ii) is operated in compliance with all applicable requirements of subchapter II of chapter 53 of title 31, United States Code (commonly referred to as the “Bank Secrecy Act”) and all other Federal anti-money laundering, anti-terrorism, and screening requirements of the Office of Foreign Assets Control and the Financial Crimes Enforcement Network.”

[897] Ibid. “The term “smart contract” means a computer protocol intended—(A) to digitally facilitate, verify, or enforce the negotiation or performance of a contract; and (B) to allow the performance of credible transactions without third parties.”

[898] Ibid. “The term “decentralized oracle” means a service that sends and verifies real world data from external sources outside of a blockchain and submits such information to smart contracts that rest on the blockchain, thus triggering the execution of predefined functions of the smart contract.”

[899] Ibid. En efecto, el proyecto define dos tipos de StableCoins: “The term “**reserve-backed stablecoin**” means a digital asset that— (A) is a representation of currency issued by the United States or a foreign government; (B) rests on a blockchain or decentralized cryptographic ledger; and (C) is collateralized on a one-to-one basis by such currency, and such currency is deposited in an insured depository institution.

The term “**synthetic stablecoin**” means a digital asset, other than a reserve-backed stablecoin, that—

(A) is stabilized against the value of a currency or other asset; and (B) rests on a blockchain or decentralized cryptographic ledger.” Los resultados son míos.

[900] Véase *supra* en 3.4.1 y en 3.3.1.1.

[901] Confr. Monetary Authority of Singapore, *A guide to digital token offerings*, recuperado el 28/04/2020 en <https://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%2>

[902] *Idem*, p. 3.

[903] *Idem*, p. 5.

[904] *Ibid.* p. 6

[905] *Supra*, 3.3.1.1.

[906] Confr. FINMA, *Regulatory treatment of initial coin offerings*, 29/09/2017, recuperado el 27/04/2020 en www.finma.ch. Se sostuvo allí: “collecting funds for one’s own account without a platform or issuing house acting as an intermediary is unregulated from a supervisory standpoint in cases where repayment is not obliged, payment instruments have not been issued and no secondary market exists.”

[907] *Ibid.*

[908] *Ibid.*

[909] *Ibid.*

[910] *Ibid.*

[911] Confr. FINMA, <https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/>, recuperado el 22/04/2020.

[912] Confr. FINMA, <https://www.finma.ch/en/finma-public/warning-list/#Order=1>, recuperado el 28/04/2020. A la fecha en que se escribe este Manual, hay 887 organizaciones incluidas en la lista sospechosa.

[913] Confr. <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>, disponible al 28/04/2020.

[914] Ibid.

[915] Ibid. Se los define como: “*payment tokens (synonymous with cryptocurrencies) are tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer.*”

[916] Ibid. Se los define como: “*Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.*”

[917] Ibid. Se los define como: “*asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. **Tokens which enable physical assets to be traded on the blockchain also fall into this category.***” El resaltado es mío.

[918] Ibid. Se los define como: “*Asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative; in other words, the tokens are deemed to be both securities and means of payment.*”

[919] Ibid. Se la define como: “*In some ICOs, tokens are already put into circulation at the point of fund-raising. This takes place on a **pre-existing blockchain**. This is referred to as pre-financing. In other types of ICO, investors are offered only the prospect that they will receive tokens at some point in the future and the tokens or the **underlying blockchain remain to be developed.***” El resaltado es mío.

[920] Ibid. Se la define como: “*Pre-sale represents another possible permutation. In this case, investors receive **tokens which entitle them to acquire other different tokens at a later date.***” El resaltado es mío.

[921] Ibid. Respecto a los utility tokens, se dijo: “*Utility tokens will not be treated as*

securities if their sole purpose is to confer digital access rights to an application or service and if the utility token can actually be used in this way at the point of issue. In these cases, the underlying function is to grant the access rights and the connection with capital markets, which is a typical feature of securities, is missing.

If a utility token additionally or only has an investment purpose at the point of issue, FINMA will treat such tokens as securities (i.e. in the same way as asset tokens)."

[922]

*Ibid. Se sostuvo: "FINMA treats asset tokens as securities. Asset tokens constitute securities within the meaning of Article 2 let. b FMIA if they represent an uncertificated security and the tokens are standardised and suitable for mass standardised trading. **An asset token also qualifies as a security if it represents a derivative** (i.e. the value of the conferred claim depends on an underlying asset) and the token is standardised and suitable for mass standardised trading. In the case of the pre-financing and pre-sale phases of an ICO which confer claims to acquire tokens in the future, these claims will also be treated as securities (i.e. in the same way as asset tokens) if they are standardised and suitable for mass standardised trading." El resultado es mío.*

[923]

Ibid, apartados 3.3-3-7.

[924]

Confr. FINMA, <https://www.finma.ch/en/news/2019/09/20190911-mm-stable-coins/>, recuperado el 27/04/2020. La caracteriza como una ICOs donde "The value of 'stable coins' is frequently linked to an underlying asset (e.g. such as fiat currency). The usual objective of such projects is to minimise the price volatility typical of currently available payment tokens. This, in turn, should increase market acceptance, in particular for payment purposes. The goal is to increase price stability compared with payment tokens such as Bitcoin or Ether. However, "stable" is primarily a marketing term." Se afirmó, además, que:

*"FINMA has found that projects to create 'stable coins' often give rise to **potential licensing requirements under the Banking Act** (BA; SR 952.0) or the **Collective Investment Schemes Act** (CISA; SR 951.31). In addition, due to their frequently intended purpose as a means of payment, the **Anti-Money Laundering Act** (AMLA; SR 955.0) is almost always applicable. If a payment system of significant importance is launched in connection with the creation of a 'stable coin', a licensing requirement under the **Financial Market Infrastructure Act** (FMIA; SR 958.1) as a payment system is probable."*

[925]

Ibid, apartados 2.2.1: "Where the token is linked to a specific fiat currency with a fixed redemption claim (e.g. 1 token = CHF 1), classification as a deposit under banking law is indicated. Where there is a redemption claim dependent on price developments, e.g. as a result of the token being linked to a basket of currencies, the distinction between a deposit under banking law and a collective investment scheme can become relevant. In this context it is important whether the underlying assets are managed for the account

and risk of the token holder (indicative of a collective investment scheme) or for the account and risk of the issuer (indicative of a deposit under banking law). For the latter categorisation to apply, all opportunities and risks from the management of the underlying assets, be they in the form of profits or losses, from interest, fluctuations in the value of financial instruments, counterparty or operational risks, must be borne by the issuer of the 'stable coin'."

[926]

Ibid, apartados 2.2.2: "Where a token is linked to commodities, the exact nature of the claim on the assets as well as the type of commodity (in particular whether "bank precious metals" or other commodities are involved) are of particular significance. **If a 'stable coin' merely evidences an ownership right of the token holder, it generally does not qualify as a security.** This presupposes that (i) an ownership right and not merely a contractual claim to the underlying commodities exists, (ii) the transfer of the token results in the transfer of the respective ownership right and (iii) the commodities are not deposited pursuant to art. 481 Code of Obligations (CO; SR 220). **Where there is merely a contractual claim against the issuer on "bank precious metals",** qualification as a deposit under banking law is probable due to the similarity to bank precious metal accounts. **Where there is a contractual claim on other commodities,** the token will generally qualify as a security and possibly as a derivative – insofar as it is linked to a financial market activity. **'Stable coins' with contractual claims on underlying assets** can therefore also give rise to a licensing requirement as a derivatives house in accordance with art. 3 para. 3 of the Stock Exchange Ordinance (SESTO; SR 954.11). Where a link to a basket of commodities (including "bank precious metals") with a price-dependent redemption claim exists, a collective investment scheme is probable." Los resultados son míos.

[927]

Ibid, apartados 2.2.3: "Where a link to individual properties or to a real estate portfolio and a redemption claim of the token holder exists, the normal third-party management of the real estate portfolio is in itself an indication of a collective investment scheme. In view of the legal hurdles involved in real estate transfers, a price-based redemption claim often exists, which also suggests a licensing requirement as a collective investment scheme."

[928]

Ibid, apartados 2.2.4: "A token that is linked to an individual security by way of a contractual right for delivery to the token holder would normally also constitute a security. Whereas a self-issuance does not generally trigger licensing requirements under the Stock Exchange Act (SESTA; SR 954.1), the acquisition and primary market offering of corresponding 'stable coins' can constitute an activity as a securities issuing company (Art. 3 para. 2 SESTO). Upon entering into force, the prospectus requirements imposed by the new Financial Services Act (FinSA; 950.1) must also be met including in cases of self-issuance. Where a link to a basket of securities with a contractual claim by the token holder on a share of the basket exists, a licensing requirement as a collective investment

scheme is probable.”

[929]

Informe disponible al 28/04/2020 en <https://www.swisslegaltech.ch/wp-content/uploads/2018/05/SLTA-Regulatory-Task-Force-Report-2.pdf>.

[930]

En efecto, el Código Suizo de las Obligaciones fue muy ponderado en el Proyecto de Código Civil del año 1999, preparado por la Comisión creada por decreto del Poder Ejecutivo Nacional 685/95, especialmente en la materia contractual, confr. el texto proyectado en <http://www.biblioteca.jus.gov.ar/ProyectoCivil-Parte1.pdf>, y su correspondiente nota de elevación, en <http://www.biblioteca.jus.gov.ar/Nota-Elevacion.PDF>, ambos disponibles al 27/04/2020. Este proyecto de Código Civil de 1999, a su turno, fue una importante fuente –sino la más importante– del anteproyecto de Código Civil y Comercial confeccionado de acuerdo a la manda del decreto presidencial 191/2011, confr. <http://www.nuevocodigocivil.com/wp-content/uploads/2015/02/5-Fundamentos-del-Proyecto.pdf> disponible al 27/04/2020.

[931]

Idem, p. 43, apartado 3.3. *“It is important to realize the limitations of smart contracts and understand that there are many elements of contractual relationship that are not suitable for performance through deterministic code embodied in a smart contract, but instead requires human judgement.”* El resaltado es mío.

[932]

Idem, p. 36, apartado 1.1.

[933]

Idem, p. 37, apartado 1.2.

[934]

Idem, p. 42, apartado 3.2.

[935]

Ibid.

[936]

Ibid. Se afirma que: *“according to Swiss case law, if the real intent of the parties cannot be determined, the judge must interpret the declarations that the parties made and their behaviors according to the principle of trust. The principle of trust means attributing the objective meaning of its declaration or behavior to a party, as the objective pursued by the parties or other circumstances might demonstrate their intent. The judge will determine the way a declaration or an attitude had to be understood according to the rules of good faith, taking into account all circumstances. Accordingly, even if one can argue that there is no explicit declaration of intent using smart contract, the behavior of a party would be sufficient to determine its intent based on the execution of the transaction. Thus, in some cases, a smart contract may be considered valid in accordance with Art. 1 para. 1 CO, depending on all facts and circumstances as well as the conduct of the parties.”* El resaltado es mío.

[937]

Idem, p. 43, apartado 3.2

[938] Ibid.

[939] Ibid.

[940] Idem, p. 44, apartado 3.3. *“What if one party did not have the legal capacity to enter into the smart contract (for instance being under age)? Swiss law provides that a contract must be entered into by a person having legal capacity to do so, e.g., a human or natural person, or a legal person such as a company. Individuals need to have the capacity to act in order to have the power to create rights and obligations through their actions in the sense of Art. 12 CC. Art. 13 CC states that a person must be over 18 years old and must, in addition, has the capacity to consent in order to have the capacity to act (Art. 14 and Art. 16 CC). A smart contract entered into by a person lacking the capacity to act, e.g. an individual being under the age of 18, will result in an invalid contract, potentially irrevocable and immutable.”*

[941] Ibid. *“If the programming code does not reflect the real intent of the parties, one could argue that there is a defect of consent, breaching Art. 1 para. 1 CO.”*

[942] Ibid. *“How can parties change self-executed obligations of the smart contract if they mutually agreed to amend the contract? As smart contracts are self-executed transaction and immutable, an amendment to the transaction is not possible.”*

[943] Ibid. *“What if the content of the smart contract is unlawful? The parties are free to decide on the content of the contract according to Art. 19 para. 1 CO. However, a contract cannot have terms that are impossible, unlawful or immoral (Art. 20 para. 1 CO). In such cases, the contract would be deemed null and void. During years, the bitcoin had the unpleasant reputation of being a tool for facilitating crimes and money laundering. As the content of the contract is unlawful according to Swiss law, such smart contracts would be considered null and void. Immorality, or the violation of bonos mores, includes the violation of personal rights or excessive contractual obligations. Thus, smart contracts lasting forever would be an issue under Swiss law as the parties’ personal freedom would be restricted excessively, therefore resulting in a violation of personality rights.”*

[944] Ibid. *“Is a contract entered with an anonymous party valid under Swiss law? Based on Art. 1 CO, one could say that both parties have expressed their mutual intent. The issue would be on how a party could enforce such contract in case of litigation.”*

[945] Idem, p. 45. *“Smart legal contracts: This term used to refer to traditional contracts, where operational elements of such contracts are represented and executed by software.”*

[946] Ibid. *“Smart contract code: This term used to refer to the code itself (known as a*

software agent) that is designed to execute certain transactions if pre-defined conditions are met.”

[947] Idem, p. 47. “In view of the conclusions reached above as regards the necessity of a universal legal drafting language at this stage in the evolution of the “smart contract” ecosystem, there does not appear any necessity or usefulness in any legal changes in the Swiss legal framework. Indeed, as discussed previously in this section, the Swiss legal framework is sufficiently robust and principles based, that it can be adapted to situations where the only representation of the agreement between two parties is a computer code on a blockchain. This presents its specific challenges, in terms of evidence production and interpretation by a court or arbitral tribunal, and should be carefully considered. However, there is no strict necessity to amend any of the Swiss law provisions dealing with contract law, whether to promote or restrict any forms of smart contracts.”

[948] Confr. Antonio Legerén-Molina, *Los contratos inteligentes en España*, en *Revista de Derecho Civil*, Vol. V, número 2, Abril-Junio 2018, p. 193.

Nótese que Legerén-Molina centra su estudio en el género de los smart legal contracts, pero sin atender a si éstos son blockchain-based, o no, que serían una especie del género. Así, precisa su enfoque sosteniendo que existe un smart legal contract, “cuando dos partes vuelcan en el código un acuerdo para que se ejecute de manera automática en el ordenador de un tercero; p. ej. un notario. Esta modalidad de contrato inteligente no tendrá en el futuro la trascendencia de los que se ejecuten utilizando dicha tecnología (en referencia a la blockchain), pero, según se verá, buena parte –por no decir todo– de lo que a continuación se expone les resulta aplicable, al responder a un esquema de funcionamiento similar. Queda, entonces, para otro momento el estudio detenido de tal subtipo de contratos inteligentes, así como de la propia tecnología de la cadena de bloques.” Confr. o.c. p. 199.

[949] Idem, p. 202. Ejemplifica Legerén-Molina otras cláusulas que tampoco podrían ser objeto de un smart legal contract: “cuando se trate de las cláusulas de exclusión de responsabilidad basadas en conductas personales o intencionales –por ejemplo, en la diligencia debida– pues tal concepto parece difícilmente reducible de manera completa a las cláusulas if/then/else y a elementos perfectamente objetivables²⁵. En el ámbito jurídico seguirá habiendo espacios donde sea necesaria la interpretación, el recurso judicial o la negociación entre las partes para apreciar si ha habido cumplimiento o incumplimiento del contrato y si surge o no la subsiguiente responsabilidad –por ejemplo, para valorar si un servicio se ha prestado de manera correcta o defectuosa–. En conclusión: no todo el espectro contractual podrá ser cubierto por smart contracts –aun cuando en los supuestos mencionados puedan establecerse para parte del contenido de tales acuerdos.”

[950] Confr. Chamber of Digital Commerce, White Paper: *Smart Contracts...* o.c. 18.

[951] Ibid., p. 19.

[952] Ibid., p. 21, nota 39.

[953] Idem, p. 211.

[954] Ibid.

[955] Véase *supra*, **nota 948**.

[956] Ibid, nota 51. Señala Legerén-Molina que, si bien no aborda en su investigación las problemáticas específicas de los blockchain-based smart contracts, “*la mayor parte de los inconvenientes que genera tal modelo de contratación inteligente se derivan fundamentalmente del uso de dicha plataforma y no tanto del propio smart contract. De entre ellos (...), cabe señalar, a modo de ejemplo, el carácter «inmutable» de los smart contracts al ser incluidos en una cadena de bloques; la eventual incompatibilidad con la legislación de protección de datos y la privacidad del contrato a la vista del carácter público de las cadenas de bloques de tal clase; o, en fin, la determinación de la normativa aplicable y la jurisdicción ante la que ventilar los eventuales conflictos, habida cuenta del carácter distribuido de la referida tecnología.*” Y agrega, en p. 98, nota 13: “*como resulta evidente, los smart contracts ejecutados en las cadenas de bloques también padecerán las dificultades que se derivan del uso de aquellas: de entrada, su incompatibilidad con el derecho al olvido (cfr. art. 17 del Reglamento UE 2016/679, de 27 de abril de 2016), su carácter pseudónimo, etc.*”

[957] Idem, p. 214. Se afirma en p. 220 que “*los caracteres que actualmente configuran el contrato inteligente no parecen exigir un nuevo Derecho de contratos, siendo perfectamente aplicables –con sus adaptaciones y modulaciones– las normas actualmente existentes. Y ello, ya estemos ante un contrato totalmente suscrito por máquinas –sería un verdadero contrato– como un contrato tradicional donde parte o todo el clausulado está escrito en el código y se ejecuta de manera automática.*” El resaltado es mío.

[958] Ibid. La norma citada dispone: “*los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez. Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.*”

[959]

Confr. Artículo 1261 del Código Civil español: “*No hay contrato sino cuando concurren los requisitos siguientes:*

- 1.º *Consentimiento de los contratantes.*
- 2.º *Objeto cierto que sea materia del contrato.*
- 3.º *Causa de la obligación que se establezca.*”

[960]

Confr. Artículo 1088 del Código Civil español: “*Toda obligación consiste en dar, hacer o no hacer alguna cosa.*”

Artículo 1088 del Código Civil español: “*El contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio.*”

[961]

Confr. Artículo 1271 del Código Civil español: “*Pueden ser objeto de contrato todas las cosas que no están fuera del comercio de los hombres, aun las futuras. Sobre la herencia futura no se podrá, sin embargo, celebrar otros contratos que aquéllos cuyo objeto sea practicar entre vivos la división de un caudal y otras disposiciones particionales, conforme a lo dispuesto en el artículo 1056. Pueden ser igualmente objeto de contrato todos los servicios que no sean contrarios a las leyes o a las buenas costumbres.*”

Artículo 1272 del Código Civil español: “*No podrán ser objeto de contrato las cosas o servicios imposibles.*”

Artículo 1273 del Código Civil español: “*El objeto de todo contrato debe ser una cosa determinada en cuanto a su especie. La indeterminación en la cantidad no será obstáculo para la existencia del contrato, siempre que sea posible determinarla sin necesidad de nuevo convenio entre los contratantes.*”

[962]

Afirma el autor citado, o.c. p. 215 que: “*en un smart contract íntegramente suscrito entre dos ordenadores por medio del que, por ejemplo, se adquieren determinados objetos o productos financieros, para las obligaciones dimanantes del contrato subsiste la misma causa sinalagmática que cuando tales prestaciones o tal acuerdo se realiza en un soporte distinto o por «personas reales». Nada obsta entonces para reconocer la existencia de una causa o razón antecedente en que se fundamenta el derecho a exigir una conducta de prestación.*”

[963]

Idem, p. 217. Señala el autor citado que será en este momento –al celebrarse el precontrato– donde deberán analizarse los vicios del consentimiento de las partes humanas o jurídicas contratantes, i.e. error, violencia, dolo, lesión. Véase *infra* en 4.5.7, donde se juzgó que el error no se puede predicar de un smart contract de trading que realizó la función programada, tal como se la programó, ya que no hay allí intervención humana alguna que pueda ser anulada por vicio de error, y las partes quedan vinculadas por el contrato, tal como se lo programó.

[964] Idem, p. 216.

[965] Ibid. Se señala que ello es posible a tenor de lo dispuesto por el Artículo 1262 del Código Civil español que reza: *“El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.*

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.” El resaltado es mío.

[966] Confr. Artículo 1278 del Código Civil español: *“Los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez.”*

Artículo 51 del Código de Comercio español: *“Serán válidos y producirán obligación y acción en juicio los contratos mercantiles, cualesquiera que sean la forma y el idioma en que se celebren, la clase a que correspondan y la cantidad que tengan por objeto, con tal que conste su existencia por alguno de los medios que el Derecho civil tenga establecidos. Sin embargo, la declaración de testigos no será por sí sola bastante para probar la existencia de un contrato cuya cuantía exceda de 1.500 pesetas,(*) a no concurrir con alguna otra prueba.*

La correspondencia telegráfica sólo producirá obligación entre los contratantes que hayan admitido este medio previamente y en contrato escrito, y siempre que los telegramas reúnan las condiciones o signos convencionales que previamente hayan establecido los contratantes, si así lo hubiesen pactado.”

[967] Confr. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Art. 23: *“Validez y eficacia de los contratos celebrados por vía electrónica.*

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la

información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.” El resaltado es mío.

[968]

Confr. Artículo 1278 del Código Civil español: “Deberán constar en documento público:

1.º Los actos y contratos que tengan por objeto la creación, transmisión, modificación o extinción de derechos reales sobre bienes inmuebles.

2.º Los arrendamientos de estos mismos bienes por seis o más años, siempre que deban perjudicar a tercero.

3.º Las capitulaciones matrimoniales y sus modificaciones.

4.º La cesión, repudiación y renuncia de los derechos hereditarios o de los de la sociedad conyugal.

5.º El poder para contraer matrimonio, el general para pleitos y los especiales que deban presentarse en juicio; el poder para administrar bienes, y de cualquier otro que tenga por objeto un acto redactado o que deba redactarse en escritura pública, o haya de perjudicar a tercero.

6.º La cesión de acciones o derechos procedentes de un acto consignado en escritura pública.

También deberán hacerse constar por escrito, aunque sea privado, los demás contratos en que la cuantía de las prestaciones de uno o de los dos contratantes exceda de 1.500 pesetas.”

[969]

Idem, p. 218. Afirma el autor citado que en tales casos, el contrato inteligente deberá cumplir con el régimen jurídico de las cláusulas generales de los contratos celebrados con consumidores contenido en la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación, y con la normativa relativa a las cláusulas no negociadas individualmente, a la información precontractual y postcontractual, y a la exigencia de entregar al consumidor una copia del contrato impresa o en soporte duradero, todo conforme al Real Decreto Legislativo 1/2007, de 16 de noviembre, de Texto Refundido de la Ley General de la Defensa de Consumidores y Usuarios.

[970]

Idem, p. 221.

[971]

Ibid. En nota 74 se afirma: “la oferta habrá de ser completa, inequívoca, reconocible, etc. Y los requisitos que tradicionalmente se reconocen a la aceptación también habrán de concurrir en el caso que se menciona: coincidencia con el contenido

de la oferta contractual, su carácter recepticio, la voluntad seria de contratar, que se realice mientras la oferta esté en vigor y no haya caducado por la razón que sea, etc.”

[972]

Ibid.

[973]

Idem, p. 222. Ilustra el punto en estos claros términos: *“Las partes celebran un contrato previo y dejan preparado el ulterior: concluyen un precontrato, condicionando la perfección del o de los futuros contratos a la concurrencia de las circunstancias preestablecidas por ellos –p. ej., determinados precios, disponibilidad, un plazo fijado, etc.(...) se trata de un pactum de contrahendo, se identifica con el contrato finalmente suscrito o es una etapa preparatoria de un iter negocial–, el caso que ahora mencionamos reúne los requisitos propios de tal figura (...) existe un acuerdo contractual inicial –hay voluntad concorde de las partes– que difiere la conclusión y entrada en vigor del o de los definitivos a un momento ulterior, caracterizado por el cumplimiento de determinadas circunstancias configuradas de manera condicional; circunstancias, que ordinariamente serán las que determinen algunos de los elementos esenciales del contrato –p. ej. cantidades, precios, etc.–. Se dejan abiertos, por tanto, los términos del precontrato, que se concretan ulteriormente, pero sin necesidad de nueva intervención específica de las partes –que ya han dado su consentimiento– al ser las propias máquinas las que efectúan tal tarea y verifican la concurrencia de las circunstancias preestablecidas (...) Entonces, cumplido el o los eventos dentro del plazo que en su caso hayan señalado –transcurrido éste sin cumplirse las condiciones, decae el precontrato–, la consecuencia que automáticamente tendrá lugar es la conclusión del o de los contratos definitivos. La automatización de lo establecido por las partes en el precontrato parece reducir, de entrada, los supuestos en que aquéllas deban compelerse –aunque pueda suceder– a concluir el proyectado contrato sujeto a condición. Lo anterior se debe a que una vez que concurren las circunstancias previstas, las máquinas concluirán de manera autónoma el contrato. No es necesario un nuevo acuerdo entre las partes pues el contenido ha quedado ya determinado o resulta determinable –aun cuando tenga carácter condicional–. Ahora bien, hasta que se verifiquen las circunstancias y se ultimen los elementos del contrato, el precontrato existente vincula a las partes, quienes, por ejemplo, han de evitar actos que supongan la frustración del contrato (...) Un ejemplo sencillo sería aquel en que las partes pactan desde el inicio una compraventa condicional, donde se subordine un número determinado de toneladas de maíz a que tengan lugar determinadas circunstancias –que el precio sea menor a determinada cantidad, que haya un excedente en tal proveedor, que los costes de transportes sean tales...–. Cuando las máquinas verifiquen por medio de dispositivos externos las condiciones preestablecidas, automáticamente cerrarán un acuerdo con el vendedor –se entiende, no en sentido físico de un ser humano pues las dos partes ya habrán codificado toda esa información–.”*

[974]

Confr. Artículo 1264 del Código Civil español: *“Será nulo el consentimiento*

prestado por error, violencia, intimidación o dolo.”

Artículo 1266 del Código Civil español: *“Para que el error invalide el consentimiento, deberá recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo.*

El error sobre la persona sólo invalidará el contrato cuando la consideración a ella hubiere sido la causa principal del mismo.

El simple error de cuenta sólo dará lugar a su corrección.”

[975]

Idem, p. 227.

[976]

Idem, p. 228. Puntualiza el autor que para el derecho español, el error sólo será invalidante cuando *“se pruebe la existencia de un error motivo –ya sea de hecho o de derecho– o de un error obstativo. Asimismo, dicho error ha de ser excusable –para no favorecer al negligente– y ha de ser manifiesto o esencial, ya sobre la sustancia, ya sobre las condiciones que se tuvieron en cuenta para prestar consentimiento; no, en cambio, cuando consista en un error de cálculo o de redacción (cfr. art. 1266 CC)”*

[977]

Idem, p. 229.

[978]

Idem, p. 230.

[979]

Confr. Artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que reza: *“1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos.”El resaltado es mío.

[980]

Confr. art. 1157 del Código Civil español: “No se entenderá pagada una deuda sino cuando completamente se hubiese entregado la cosa o hecho la prestación en que la obligación consistía.”

[981] Confr. art. 1169 del Código Civil español: “A menos que el contrato expresamente lo autorice, no podrá compelerse al acreedor a recibir parcialmente las prestaciones en que consista la obligación.

Sin embargo, cuando la deuda tuviere una parte líquida y otra ilíquida, podrá exigir el acreedor y hacer el deudor el pago de la primera sin esperar a que se liquide la segunda.”

[982] Idem, p. 232.

[983] Idem, p. 233. Se afirma que “El automatismo propio de los contratos inteligentes, cuya ejecución no depende de la voluntad humana de las partes, no impide, pero dificulta, que se dé un pago por tercero. En efecto, es posible que un tercero realice la prestación a favor del deudor de forma que satisfaga su interés, pero lo que previsiblemente ocurrirá entonces es que se efectúe un doble pago (...) la propia estructura de los contratos inteligentes dificulta también que se efectúe un pago a favor de un acreedor aparente: no parece sencillo que exista otro que esté «en posesión del crédito» (...) Es también el carácter automático el que impide, de entrada, el pago por cesión de bienes o la dación en pago (...)

En sentido parecido, el automatismo en la ejecución de las prestaciones priva de sentido al mecanismo del ofrecimiento de pago y la consignación en esta modalidad contractual. Y algo similar sucede respecto de la imputación de pagos: al ser automático el pago, se dificulta la existencia de supuestos donde quepa la referida imputación –si, por hipótesis, pudiera darse, se aplicarían los criterios generales (art. 1172 y 1174 CC)–. Lo anterior no impide que pueda suscribirse un smart contract específico para la gestión de las imputaciones de pagos o las compensaciones de deudas entre determinadas partes.”

[984] Se sigue en este apartado, en general, a Ken Kawai y Takeshi Nagase, *The Virtual Currency Regulation Review 2: Japan*, disponible al 28/04/2020 en <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-2/1197588/japan> y a So Saito y Joerg Schmidt, *Digital assets in Japan*, recuperado el 29/04/2020 en https://innovationlaw.jp/wp/wp-content/uploads/2020/03/digital_assets_JP_final.pdf.

[985] Confr. Ken Kawai y Takeshi Nagase, *Japan: Blockchain*, recuperado el 28/04/2020 en <https://www.legal500.com/guides/chapter/japan-blockchain/?export-pdf>.

[986] Confr. <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow>, disponible el 28/04/2020.

[987] Confr. <https://news.bitcoin.com/cryptocurrency-exchanges-japan/> disponible el 28/04/2020.

[988] Confr. la Asociación Japonesa de Casas de Cambio de Monedas Virtuales (JVCEA, en inglés), véase <https://medium.com/@newscnofficial/the-japan-virtual-currency-exchange-association-jvcea-japans-official-self-regulatory-body-341d6e2817e8>, recuperado el 28/04/2020. Véase también su website

[989] Confr. <https://news.bitcoin.com/japan-cryptocurrency-industry-self-regulation/> disponible al 15/05/2020.

[990] Confr. Ken Kawai y Takeshi Nagase, *Japan: Blockchain*, o.c., apartado 5.

[991] Confr. <https://www.ft.com/content/b8360e86-aceb-11e7-aab9-abaa44b1e130>, recuperado el 28/04/2020. En Diciembre de 2013, China prohibió a sus bancos y entidades de pago que operaran con monedas virtuales, permitiendo el *trading* a los *Exchanges* chinos, regulándose la actividad por parte de la Agencia Reguladora de las Telecomunicaciones. En 2017 se prohibió la emisión de ICOs y se prohibió también la actividad de los *Exchanges*. La prohibición total se basó principalmente en la imposibilidad de prevenir el lavado de activos a través de monedas virtuales.

[992] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan*, recuperado el 29/04/2020 en https://innovationlaw.jp/wp/wp-content/uploads/2020/03/digital_assets_JP_final.pdf, p. 2.

Señalan los autores citados que el Artículo 2(5)(i) de la ley de servicios de pago los define como: “*property value that can be (i) used with unspecified persons for purchasing goods or services, (ii) purchased from and sold to unspecified persons acting as counterparty, and (iii) transferred electronically.*”

[993] Ibid. Señalan los autores citados que el Artículo 2(5)(ii) de la ley de servicios de pago los define como: “*property values that can be (i) mutually exchanged with type I crypto assets with unspecified persons acting as a counterparty and (ii) transferred electronically.*”

[994] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan*, recuperado el 29/04/2020 en https://innovationlaw.jp/wp/wp-content/uploads/2020/03/digital_assets_JP_final.pdf, p. 2.

[995] Confr. So Saito y Joerg Schmidt, *Stable Coins under Japanese law*, recuperado el 29/04/2020 en https://innovationlaw.jp/wp/wp-content/uploads/2019/06/ENstable_coin_article_190621.pdf.

[996] Véase *supra*, nota 421.

[997] Véase *supra*, nota 421. Ampliar en <https://news.bitcoin.com/coincheck-halts-operations-amidst-hacking-rumors-after-723-million-withdrawn/> disponible al

28/04/2020.

[998] Véase <https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft>, recuperado el 28/04/2020.

[999] Confr. *Report from Study Group on Virtual Currency Exchange Services*, 12/12/2018, disponible al 28/04/2020 en: <https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181221-1.pdf>.

[1000] Confr. Anderson Mori & Tomotsune, *Revisions to Payment Services Act provisions, etc. on crypto assets*, recuperado el 28/04/2020 en https://www.amt-law.com/asset/pdf/bulletins2_pdf/190523.pdf.

[1001] Confr. <https://www.cryptopolitan.com/crypto-regulations-in-japan/> recuperado el 28/04/2020.

[1002] Confr. https://medium.com/@missbitcoin_mai/new-blockchain-trends-on-japanese-market-10cd9a3da46b, recuperado el 29/04/2020.

[1003] Véase supra, en § 3.3.1.6.

[1004] Confr. Ken Kawai y Takeshi Nagase, *Japan: Blockchain..o.c.*, p. apartado 2.

[1005] Confr. *Report from Study Group on Virtual Currency Exchange Services*, 12/12/2018, disponible al 28/04/2020 en: <https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181221-1.pdf>

[1006] Confr. Ken Kawai y Takeshi Nagase, *The Virtual Currency Regulation Review 2: Japan* o.c. Véase también Marie Huillet, *Japan officially approves bill to amend national legislation governing crypto regulation*, disponible al 28/04/2020 en <https://cointelegraph.com/news/japan-officially-approves-bill-to-amend-national-legislation-governing-crypto-regulation>.

[1007] Confr. Marie Huillet, *Japan officially approves bill to amend national legislation governing crypto regulation*, disponible al 28/04/2020 en <https://cointelegraph.com/news/japan-officially-approves-bill-to-amend-national-legislation-governing-crypto-regulation>

[1008] Confr. Adrian Zmudzinski, *Japan: crypto may be classified as “crypto-assets” to prevent confusión with legal tender*, disponible al 22/04/2020 en <https://cointelegraph.com/news/japan-crypto-classified-as-crypto-assets-to-prevent-confusion-with-legal-tender>.

[1009] Confr. Ken Kawai, Akihito Miyake, Shunsuke Aoki, Tomoyuki Tanaka, Takeshi Nagase y Keisuke Hayashi, *Revisions to Payment Services Act Provisions, etc.*

on crypto assets, disponible al 28/04/2020 en https://www.amt-law.com/asset/pdf/bulletins2_pdf/190523.pdf, apartado 2-1, p. 4.

[1010]

Confr. So Saito y Joerg Schmidt, *Digital assets in Japan...o.c.*, p. 23. Se la define en estos términos: “*The term crypto asset management is understood broadly and covers any activity where a service provider controls the crypto assets of another party. In cases in which the service provider holds the private key(s) of a user, and is able to initiate a transfer of the crypto assets, the services constitute crypto asset management services within the meaning of the PSA and are subject to registration.*”

[1011]

Ibid. Se sostiene allí que: “*Crypto asset custodians as defined above must not only manage the crypto assets of their users separately from their own, but also separately from the other users’ assets to allow easy identification. **The private keys controlling the users’ crypto assets must generally be managed via devices which are permanently disconnected from the internet or by other methods that provide a similar level of security.** Crypto assets which are held in hot wallets, i.e. where the private keys are stored on devices that are permanently connected to the internet, must be backed by the custodian’s own funds. Under the PSA, **custodians are required to hold the same amount of the same crypto asset as their own assets in a cold wallet or in a wallet secured by a method providing a similar level of security, as the funds stored in a hot wallet. The same applies to crypto asset exchanges, which manage their users’ crypto assets.***” Los resaltados son míos.

[1012]

Confr. So Saito y Joerg Schmidt, *Digital assets in Japan...o.c.*, p. 5.

[1013]

Idem, p. 6. Para poder obtener licencia de Exchange en Japón: “*companies must be incorporated as a stock company and have a minimum capital of JPY 10 million. An exchange must further ensure that its net assets do not fall below the amount of users’ funds that are stored in a hot wallet. Aside from this, crypto asset exchanges must implement corporate governance and security systems that ensure fair dealing on the exchange and reduce operational risks. The latter includes the separation of funds – both for crypto assets and fiat currencies– and the proper management of users’ funds held by the exchange. Crypto asset exchanges violating their obligations under the PSA are subject to fines of up to JPY 3 million*”

[1014]

Ibid. Para ofrecer tokens de terceros, los Exchanges deben analizar varios aspectos críticos del emisor del ICOs: “*including the issuer’s financial statements, material agreements, business plan, whitepaper, and other documents deemed necessary by the issuer.*” Debe destacarse que la Asociación Japonesa de Casas de Cambio de Monedas Virtuales debe *pre-aprobar* cualquier oferta de una ICO en Japón. Una vez autorizada la venta de una ICOs, “*an issuer must disclose a wide variety of information to the public in order to allow investors to make an informed decision. This includes*

among others: information on the issuer, information on the tokens and the token sale (incl. pricing information, incentives, sales period, token allocation, caps, future distributions), information on the use and the accounting treatment of the raised funds, information on the Project, governing law and jurisdiction.

Once the ICO is completed, the issuer must provide token holders with sales data, including information on the number of tokens issued and the total amount collected. Token issuers are further subject to ongoing disclosure and must publish data about the status of the project and market value of the tokens at regular intervals. This generally applies **for a period of five years** unless the protection of users is not compromised, and the issuer has informed the JVCEA. An issuer may not use the raised funds for any other purpose than disclosed to investors during the ICO and must manage them separately from its other funds. **The private key controlling the raised funds must generally be stored offline.** The issuer must further establish an internal control system to prevent the misappropriation of funds by its officers and employees or the theft by third parties.” Los resultados son míos.

[1015] Ibid.

[1016] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan...o.c.*, p. 8.

[1017] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan...o.c.*, p. 24, se afirma que: “With respect to exchanges managing their users’ fiat money, they must store these funds separately from their own funds with a trust. In case of insolvency, the funds, both crypto and fiat, are protected, and users of the crypto asset exchange are given priority over the other creditors.”

[1018] Confr. Mitsuharu Kataoka y Takanobu Morita, *Digital Securitization of Real Estate - Recent Amendments to the Financial Instruments and Exchange Act of Japan*, recuperado el 29/04/2020 en <https://www.dlapiper.com/en/australia/insights/publications/2020/04/re-digital-securitization-japan-updates-to-financial-instruments/>.

[1019] Ibid. Se sostiene que “ERTRs can have high assignability as a result of the use of an electronic data processing system (such as digital tokens), and as a result ERTRs are treated as Paragraph 1 Securities to which stricter regulations apply in order to protect investors.”

Confr. So Saito y Joerg Schmidt, *Digital assets in Japan..o.c.* sostienen que la ley de Instrumentos Financieros y Casas de Cambio “distinguishes between type I and type II securities. Type I securities are traditional securities such as bonds and stocks, which are generally perceived as being highly liquid. Type II securities are, for example, units in a fund, beneficial interests in a trust, membership rights in a general partnership or limited partnership, and equity in limited liability companies. These securities are

generally much less liquid than type I securities and are therefore subject to lighter regulation. With the occurrence of tokenization, type II securities became, however – at least in theory – much more liquid. As a response, the legislator introduced electronically recorded transfer rights into the Financial Instruments and Exchanges Act. These rights represent type II securities which are treated as type I securities”.

[1020] Ibid.

[1021] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan*.o.c. afirman que no serán considerados ETRTs porque “*there must not be any liquidity constraints or other circumstances specified by cabinet order. Tokens that are sold to professional investors and for which the transferability is technically restricted*”.

[1022] Ibid. Citan como ejemplo: “*a digital token technically may not be assigned to another person other than a **qualified institutional investor** or other **investors who are considered to have appropriate investment knowledge**; and (ii) each **assignment** of such digital tokens **requires** an application by the assignor for **approval** by the issuer and approval by the issuer.*” El resaltado es mío

[1023] Ibid. Precisan los autores citados: “*If solicitations are made to 50 or more investors for an offering or a secondary distribution of ETRTs, and unless the requirements for **private placements** (either with QIIs, with special investors, or with a small number of investors) are met, issuers of ETRTs are required to file with the relevant authority a securities registration statement and must also issue a related prospectus.*”El resaltado es mío.

[1024] Ibid.

[1025] Ibid. Aclaran los autores citados: “***Issuers of ETRTs** representing **CISIs** are now required to register as a Type 2 Financial Instrument Business Operator unless they use a licensed business operator to handle solicitations of such ETRTs or themselves meet the requirements for a Specifically Permitted Business for QIIs which include, without limitation, (i) investors include at least one QII, (ii) the number of the other non-QII investors are 49 or less and (iii) such other non-QII investors are considered to have appropriate investment knowledge or closely related to the issuer. **A person who handles solicitations** of ETRTs on behalf of the issuer is required to be registered as a Type 1 Financial Instrument Business Operator since ETRTs are classified as Paragraph 1 Securities.*

***CISIs** are interests in an investment scheme satisfying the following criteria:(i) the investors invest or contribute cash or other assets to a business through a partnership, silent partnership, or the like; (ii) the investors have the right to receive dividends of profits or assets obtained from the business; and (iii) any of the exemptions (e.g., cases in which all the investors are involved in operation or management of the business not just*

making investment in the business) does not apply to the investment scheme.” El resaltado es mío.

[1026]

En la República Argentina, los contratos derivados fueron regulados por la Ley 27.440 (B.O. 11/05/2018), en sus Artículos 188 a 194, asignándose a la Comisión Nacional de Valores la facultad de regulación y aplicación del régimen. Allí se los definió a los contratos de derivados como: “*contratos (i) sujetos a la ley y jurisdicción argentina o extranjera y celebrados bajo acuerdos marcos, individuales y/o bajo los términos y condiciones establecidos por el mercado en el que se concerten; (ii) en los cuales sus términos y condiciones, incluyendo precio, cantidad, garantías y plazo, derivan o dependen de un activo o producto subyacente, los que pueden consistir, a modo enunciativo, en: (a) activos financieros, tasas de interés o índices financieros, (b) valores negociables y/o (c) activos no financieros (incluyendo a modo enunciativo cereales, minerales, alimentos, inmobiliarios); (iii) que se pueden celebrar y/o negociar en mercados autorizados por la Comisión Nacional de Valores o fuera de los mismos; y (iv) que incluyen, a modo enunciativo, los contratos a término, (denominados en idioma inglés "forwards"), los contratos de futuros (denominados en idioma inglés "futures"), los contratos de opciones (denominados en idioma inglés "options"), los contratos de intercambios (denominados en idioma inglés "swaps") y los derivados de crédito (incluyendo los denominados en idioma inglés "credit default swaps"), y/o una combinación de todos o alguno de ellos.”*

También se definió a los márgenes y garantías como: “*contratos (i) sujetos a la ley y jurisdicción argentina o extranjera y celebrados mediante acuerdos marcos o individuales o según las reglamentaciones de los mercados autorizados por la Comisión Nacional de Valores, mediante los cuales las contrapartes o terceros acuerdan la entrega de valores negociables, activos financieros, dinero, moneda que no sea de curso legal en la República Argentina y cualquier otra cosa mueble, con la finalidad de asegurar el cumplimiento de cualquier clase de obligaciones de pago y entrega bajo los Derivados y Pases.”*

[1027]

Confr. Emmanuel Goh, *Crypto derivatives: A corner of the market or the market itself?* Recuperado el 28/04/2020 en <https://www.coindesk.com/crypto-derivatives-a-corner-of-the-market-or-the-market-itself>.

[1028]

Ibid.

[1029]

Ibid, citando a Warren Buffet.

[1030]

Confr. <https://www.fca.org.uk/news/press-releases/fca-proposes-ban-sale-crypto-derivatives-retail-consumers>, recuperado el 28/04/2020. Sostien desde la FCA que “*these products are ill-suited to retail consumers who cannot reliably assess the value and risks of derivatives or Exchange Traded Notes that reference certain*

cryptoassets (crypto-derivatives). This is due to: (i) inherent nature of the underlying assets, which have no reliable basis for valuation, (ii) the prevalence of market abuse and financial crime in the secondary market for cryptoassets (eg cyber theft), (iii) extreme volatility in cryptoasset prices movements, and (iv) inadequate understanding by retail consumers of cryptoassets and the lack of a clear investment need for investment products referencing them. These features mean retail consumers might suffer harm from sudden and unexpected losses if they invest in these products. **The FCA is therefore consulting on banning the sale, marketing and distribution to all retail consumers of all derivatives (ie contract for difference - CFDs, options and futures) and ETNs that reference unregulated transferable cryptoassets by firms acting in, or from, the UK.**” El resaltado es mío.

[1031] Confr. Emmanuel Goh, *Cyrpto derivatives: A corner...o.c.*

[1032] Confr. Hisashi Oki, *Japan hopes to set global crypto law benchmark with latest regulatory update*, recuperado el 28/04/2020 en <https://cointelegraph.com/news/japan-hopes-to-set-global-crypto-law-benchmark-with-latest-regulatory-update>. Véase también So Saito y Joerg Schmidt, *Digital assets in Japan..o.c.*, p. 4.

[1033] Confr. Emmanuel Goh, *Cyrpto derivatives: A corner...o.c.* Quien afirma que ello ya ocurrió en Mayo de 2019, confr. <https://www.zerohedge.com/news/2019-05-17/what-caused-last-nights-bitcoin-flash-crash>, recuperado el 28/04/2020.

[1034] Confr. So Saito y Joerg Schmidt, *Digital assets in Japan..o.c.* p. 22.

[1035] Confr. Marie Huillet, *Japan officially approves bill to amend national legislation governing crypto regulation*, disponible al 28/04/2020.

[1036] Confr. Ken Kawai, Akihito Miyake y otros, *Revisions to Payment Services Act Provisions..o.c.*

[1037] Confr. Ken Kawai, Akihito Miyake y otros, *Revisions to Payment Services Act Provisions..o.c.*, indican que la reforma “also prohibit a Crypto Asset Exchange Service Provider or any of its officers from engaging in any of the following: (i) making any misrepresentation or representation under a Crypto Asset Exchange Agreement that is likely to lead to an inaccurate understanding of the nature or any other aspects of a crypto asset; (ii) making any misrepresentation or representation in an advertisement concerning a Crypto Asset Exchange Service that is likely to lead to an inaccurate understanding of the nature or any other aspects of a crypto asset; (iii) making a representation under a Crypto Asset Exchange Agreement or in an advertisement concerning a Crypto Asset Exchange Service, to induce the sale or purchase of a crypto asset or the exchange of a crypto asset for another crypto asset that is (a) not for the

purpose of using the relevant crypto asset as a means of payment, but (b) for the exclusive purpose of promoting the interests in a particular crypto assets; (iv) Such other acts specified in the relevant Cabinet Office Ordinance as being likely to result in (a) insufficient protection of Crypto Asset Exchange Service users or (b) inappropriate performance or inadequate security in the performance of any Crypto Asset Exchange Service. Any person at a Crypto Asset Exchange Service Provider who engages the act referred to in **item (ii) or (iii)** above is **punishable by imprisonment for a term not exceeding six (6) months** or a fine not exceeding JPY500,000, or both.¹⁸ Additionally, juridical persons (including corporations) are also subject to dual liability for such acts and are punishable by a fine not exceeding JPY500,000.” El resaltado es mío.

[1038]

Confr. Ken Kawai, Akihito Miyake y otros, *Revisions to Payment Services Act Provisions*..o.c.

[1039]

Confr. Ministry of Economy, Trade and Industry, *Survey on Technology and Institution related to Distributed system*, Marzo de 2018, recuperado el 28/04/2020 en https://www.meti.go.jp/english/press/2018/pdf/0723_001a.pdf.

[1040]

Ibid.

[1041]

Ibid., apartado 3.2

[1042]

Confr. <https://cointelegraph.com/news/south-korean-government-bans-officials-from-crypto-holding-and-trading> recuperado el 28/04/2020.

[1043]

Confr. Skalex, *Crypto in South Korea: a History and What's next?* Recuperado el 28/04/2020 en <https://www.skalex.io/crypto-south-korea/>

[1044]

Confr. <https://thenews.asia/amendment-to-special-reporting-act-passes-cryptocurrency-trading-now-legal-in-south-korea/>, recuperado el 28/04/2020.

[1045]

Confr. Paddy Baker, *South Korea's Central Bank is building a new blockchain ecosystem for the bond market*, recuperado el 28/04/2020 en <https://www.coindesk.com/south-koreas-central-bank-is-building-a-new-blockchain-system-for-the-bond-market>.

[1046]

Ibid.

[1047]

Confr. Daniel Kuhn, *South Korean Central Bank to organize a CBDC task force*, recuperado el 28/04/2020 en <https://www.coindesk.com/south-korean-central-bank-to-organize-a-cdbc-task-force>.

[1048]

Confr. <https://techcrunch.com/2018/04/03/s-coin/>, recuperado el 28/04/2020.

[1049]

Confr. <https://thecryptocurrencypost.net/south-korea-launches-s-coin-token->

[for-residents-of-the-capital/](#), recuperado el 28/04/2020.

[1050] Ibid.

[1051] Confr. http://www.fsc.go.kr/eng/new_press/releases.jsp, recuperado el 27/04/2020. El regulador coreano dispuso que: *“Under the new rule, users who want to make cryptocurrency transactions must have a bank account under their real name at the same bank with cryptocurrency exchanges. Those who do not have their real-name account at the same bank will only be allowed to withdraw money from their existing bank account. To make new deposits, they are required to open a new bank account under their real name at the same bank with the exchanges.”*

[1052] Confr. <https://www.coinspeaker.com/south-korea-bans-raising-money-icos-bitcoin-ether-prices-fall/> recuperado el 28/04/2020.

[1053] Ibid.

[1054] Confr. Skalex, *Crypto in South Korea: a History and What’s next?* Recuperado el 28/04/2020 en <https://www.skalex.io/crypto-south-korea/>

[1055] Confr. <https://www.forbes.com/sites/elaineramirez/2018/01/23/why-south-korea-is-banning-all-foreigners-from-trading-cryptocurrency/#571bed7e7345> recuperado el 28/04/2020.

[1056] Confr. <https://cointelegraph.com/news/south-korean-government-bans-officials-from-crypto-holding-and-trading> recuperado el 28/04/2020.

[1057] Confr. <https://cointelegraph.com/news/south-korea-govt-officials-accused-of-crypto-insider-trading> recuperado el 28/04/2020.

[1058] Confr. http://www.fsc.go.kr/eng/new_press/releases.jsp, recuperado el 28/04/2020.

[1059] Confr. http://www.fsc.go.kr/eng/new_press/releases.jsp, recuperado el 28/04/2020.

[1060] Confr. <https://www.lexology.com/library/detail.aspx?g=dd7ef79a-5c8d-4462-963f-229db56435fd> recuperado el 28/04/2020.

[1061] Confr. http://www.leeko.com/newsl/fintech/1912/fin1912_e.html, recuperado el 28/04/2020.

[1062] Confr. <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3075266>, recuperado el 28/04/2020.

[1063] Confr. Danny Crichton, *South Korea passes one of the world's first comprehensive cryptocurrency laws*, recuperado el 28/04/2020 en <https://techcrunch.com/2020/03/05/south-korea-passes-one-of-the-worlds-first-comprehensive-cryptocurrency-laws/>. Ampliar también en <https://en.cryptonist.ch/2020/03/09/south-korea-crypto-regulation-coronavirus/> disponible al 28/04/2020 y en <https://dailyhodl.com/2020/03/08/south-korea-passes-landmark-legislation-to-legalize-and-regulate-cryptocurrency-and-exchanges/>, recuperado el 28/04/2020.

[1064] Confr. <http://www.koreaitimes.com/news/articleView.html?idxno=87177>, recuperado el 28/04/2020.

[1065] Confr. <https://www.coinspeaker.com/france-introduces-new-ico-framework-to-become-europes-ico-hub/>, recuperado el 28/04/2020.

[1066] Confr. Robert Ophèle, Presidente de la AMF, 20 de Noviembre de 2019, Bruselas, disponible al 29/04/3030 en <https://www.amf-france.org/en/news-publications/public-statements/speech-robert-ophele-amf-chairman-ecsda-annual-conference-20-november-2019-brussels>.

[1067] Para ver todos los asuntos incluidos en la ley, véase <https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation>, disponible al 28/04/2020.

[1068] Confr. <https://world.businessfrance.fr/nordic/wp-content/uploads/sites/903/2016/04/The-Business-Growth-and-Transformation-Action-Plan-PACTE-in-ten-measures.pdf>, recuperado el 28/04/2020.

[1069] Existe una regulación específica de la AMF sobre el contenido del White Paper, disponible aquí: https://doctrine.amf-france.org/en_US/Reglementation/Doctrine/Doctrine-list/Doctrine?xtcr=1&isSearch=true&docId=workspace%3A%2F%2FspacesStore%2Faf1f24bd-6d7b-4386-aa4b-f1fb69ea877f&lastSearchPage=https%3A%2F%2Fwww.amf-france.org%2FmagnoliaPublic%2Famf%2FResultat-de-recherche%3FTEXT%3DDOC-2019-06%26LANGUAGE%3Dfr%26isSearch%3Dtrue%26simpleSearch%3Dtrue%26valid_recherche%3FTEXT%3DDOC-2019-06&docVersion=1.0&docVersion=1.1&langSwitch=true al 28/04/2020.

[1070] Confr. <https://www.soulier-avocats.com/en/pacte-bill-a-framework-for-icos-and-protection-of-foreign-investments-in-france/>, recuperado el 28/04/2020.

[1071] Ibid.

[1072] Ibid.

[1073] Ibid.

[1074] Confr. <https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/amf-grants-its-first-optional-approval-initial-coin-offering-ico> disponible al 28/04/2020.

[1075] Ibid.

[1076] Confr. AMF, *Review and analysis of the application of financial regulations to security tokens*, 27/02/2020, recuperado el 28/04/2020 en https://www.amf-france.org/sites/default/files/2020-03/legal-analysis-security-tokens-amf-en_1.pdf. En este estudio, se indica que Alemania y Holanda también han levantado el punto de que se requieren modificaciones legislativas. Se señala el caso de Lituania y de Suiza como los más avanzados en materia regulatoria de STOs en Europa.

[1077] Ibid.

[1078] Ibid. p. 8, se citan estos casos: “**Société Générale** (Forge project): the Société Générale group issued a first STO for an amount of at least €100m finalised on 18 April 2019 concerning housing financing bonds (refinancing vehicle for group housing mortgage loans), subscribed to entirely within the group. It can therefore not be classified as a public offer and is not covered by a prospectus; **Nebulous** (Sia Funds): STO issuance finalised in April 2018 concerning financial instruments giving entitlement to a stake in the company and in the revenue generated by its business (decentralised storage platform based on the blockchain technology). The operation took place in the form of a private placement open only to qualified investors; **Carthagea**: STO issuance made in March 2019 concerning shares designed to finance nursing homes for the elderly in Tunisia. It is made by a French project promoter to French investors subscribing for at least €100,000. Under current law it is therefore not considered as a public offer and is not covered by a prospectus; **Monali**: STO issuance carried out on September 5, 2019, with the objective of raising € 2 million. As its amount is less than € 8 million, it is not subject to the obligation to submit a prospectus to the AMF. Furthermore, the offer was open only to qualified investors; **Authenticao**: STO issuance carried out on October 10, 2019, with the objective of raising € 7.9 million, open only to qualified investors; **Kay Flo**: STO issuance carried out on October 15, 2019, with the objective of raising € 2.1 million, open only to qualified investors; **Sky Spring**: STO issuance carried out on November 12, 2019, with the objective of raising € 8.8 million, open only to qualified investors.” (el resultado es mío).

[1079] Ibid, p. 11.

[1080]

Ibid., p. 14. Se indica que las plataformas de *trading* pueden asumir tres formas: (i) peer-to-peer o OTC Exchange platforms, donde las transacciones son bilaterales entre token holders; (ii) modelo broker-dealer, donde la plataforma puede actuar por cuenta y nombre propio, o intermediar por cuenta de terceros; y (iii) sistema multilateral, donde hay un agente central que garantiza las operaciones que se realizan, o puede operar descentralizadamente on-chain, o ser un modelo híbrido, semi-centralizado.

[1081]

Confr. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A124036e> recuperado el 28/04/2020.

[1082]

Ibid., p. 18. *“There is no blockchain manager because of the decentralised nature of the blockchain, which inherently implies no legal link or shared responsibility between participants. The absence of a manager also makes it difficult to apply the European Regulation on market abuse. However, if a public blockchain does not have a manager identifiable by its decentralized nature, this does not mean that the trading platform that uses this blockchain has not either. In addition, while the most widespread and widely used token standards to date, such as the ERC20 standard, do not allow a defined manager to exercise control over transactions, many teams are working on suitable token standards to those needs. Thanks to these new standards, it would be possible in particular to prevent an address from sending tokens over a given period, to put on a white list the Ethereum addresses that can receive the token (after KYC), to prevent addresses at expired KYC to make transactions, to define sending and receiving limits or to give control rights to third parties.”* El resaltado es mío.

[1083]

Confr. <https://www.securities-services.societegenerale.com/en/insights/views/news/pacte-bill-french-regulatory-regime-crypto-asset-service-providers/>, recuperado el 28/04/2020.

[1084]

Ibid.

[1085]

Ibid.

[1086]

Ibid.

[1087]

El texto de la ley puede encontrarse, al 05/05/2020 en http://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018.

[1088]

Confr. <https://www.criptonoticias.com/mercados/casas-cambio-chilenas-esperan-reapertura-cuentas-bancarias-proximos-dias/>, <https://www.t13.cl/noticia/negocios/tdlc-rechazo-apelaciones-bancoestado-e-itau-no-reabrir-cuentas-empresas-criptomonedas>, <https://www.latercera.com/la-tercera->

[pm/noticia/casa-criptomonedas-eleva-disputa-bancos-exige-ineditas-multas-cierre-cuentas-corrientes/139277/](https://www.elpaese.cl/actualidad/2020/05/03/pm/noticia/casa-criptomonedas-eleva-disputa-bancos-exige-ineditas-multas-cierre-cuentas-corrientes/139277/)

disponibles al 03/05/2020.

[1089]

Confr. caso **CryptoMKT** SpA, disponible al 04/05/2020 <https://consultas.tdlc.cl/download/146012?inlineifpossible=true> y caso **Orionx** SpA, disponible al 04/05/2020 en <https://consultas.tdlc.cl/download/146785?inlineifpossible=true>.

[1090]

Confr. <https://www.emol.com/noticias/Economia/2019/02/08/937234/Banco-Central-envia-oficio-al-TDLC-con-duras-criticas-a-las-criptomonedas-en-medio-del-conflicto-con-los-bancos.html> disponible al 03/05/2020. La posición del Banco Central de Chile está disponible, al 03/05/2020 en este link: https://consultas.tdlc.cl/do_search?proc=3&idCausa=42108

[1091]

Confr. Causa: C-385-2019 P Medida prejudicial cautelar solicitada por **ARCADI** SpA., en contra de BANCO SANTANDER-CHILE, y decisión del TDLC de fecha 13/01/2019 disponible al 03/05/2020 en <https://consultas.tdlc.cl/download/169287?inlineifpossible=true>.

[1092]

Confr. <https://www.criptonoticias.com/gobierno/regulacion/corte-suprema-chile-avala-cierre-cuentas-bancarias-orionx/> disponible al 04/05/2020 y <https://thecryptolegal.com/el-tribunal-antimonopolio-chileno-contradice-a-la-corte-suprema-de-chile-sobre-la-apertura-de-cuentas-bancarias-para-empresas-de-criptomonedas/>, disponible a la misma fecha.

[1093]

Información sobre el caso disponible en <https://oficinajudicialvirtual.pjud.cl/indexN.php#modalDetalleSuprema> y https://oficinajudicialvirtual.pjud.cl/ADIR_871/suprema/documentos/docCausaSuprevalorFile=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvbnZRPbuJbz6k disponible al 03/05/2020.

[1094]

Confr. Sebastián J. Cosola y Walter C. Schmidt, *Coexistencia de dos mundos. El impacto del mundo digital en el ordenamiento jurídico*, Revista del Notariado, N° 935, Enero-Marzo 2019, disponible al 29/04/2020 en http://www.revista-notariado.org.ar/wp-content/uploads/2019/11/RDN_935_pdf.pdf, p. 102.

[1095]

Confr. Robby Houben y Alexander Snyers, *Crypto-assets*, disponible al 28/04/2020 en [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU\(2020\)0171_en.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)0171_en.pdf) p. 17.

[1096]

Idem, p. 17.

[1097] Idem, p.103.

[1098] Confr. Robby Houben y Alexander Snyers, *Crypto-assets,...o.c.*, p. 18.

[1099] Confr. Santiago Mora, *El sistema Bitcoin y las criptomonedas en el derecho argentino*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed. CDYT, 2019, Buenos Aires, p. 97.

[1100] “Art. 772, CCCN.- *Cuantificación de un valor. Si la deuda consiste en cierto valor, el monto resultante debe referirse al valor real al momento que corresponda tomar en cuenta para la evaluación de la deuda. Puede ser expresada en una **moneda sin curso legal que sea usada habitualmente en el tráfico**. Una vez que el valor es cuantificado en dinero se aplican las disposiciones de esta Sección.*”

[1101] Véase <https://makerdao.com/es/>

[1102] “Art. 1, CCCN.- *Fuentes y aplicación. Los casos que este Código rige deben ser resueltos según las leyes que resulten aplicables, conforme con la Constitución Nacional y los tratados de derechos humanos en los que la República sea parte. A tal efecto, se tendrá en cuenta la finalidad de la norma. Los usos, prácticas y costumbres son vinculantes cuando las leyes o los interesados se refieren a ellos o en situaciones no regladas legalmente, siempre que no sean contrarios a derecho.*”

[1103] “Art. 765, CCCN.- *Concepto. La obligación es de dar dinero si el deudor debe cierta cantidad de moneda, determinada o determinable, al momento de constitución de la obligación. Si por el acto por el que se ha constituido la obligación, **se estipuló dar moneda que no sea de curso legal en la República**, la obligación debe considerarse como de dar cantidades de cosas y el deudor puede liberarse dando el equivalente en moneda de curso legal.*” El resaltado es mío.

[1104] Confr. Santiago Mora, *La tecnología blockchain: contratos inteligentes, ofertas iniciales de monedas y demás casos de uso*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed. CDYT, 2019, Buenos Aires, p. 132, nota 54.

[1105] Ibid.

[1106] Véase *supra*, § 3.4.1.3.1.5.

[1107] Véase *supra*, § 3.4.2.2.2.

[1108] Véase *supra*, § 3.4.8.1.

[1109] Confr. Ignacio Alterini, *Los fundamentos del derecho real*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo VI, Buenos Aires, 2016, p. 3.

[1110] Confr. Art. 1883, CCCN, que reza: “Objeto. El derecho real se ejerce sobre la totalidad o una parte material de la **cosa** que constituye su objeto, por el todo o por una parte indivisa. El objeto también puede consistir en un **bien** taxativamente señalado por la ley.” El resaltado es mío.

[1111] Confr. Art. 16, CCCN. Afirman esta relación, Renato Rabbi-Baldi Cabanillas y Ernesto Solá, en Código Civil y Comercial de la Nación Comentado, Julio César Rivera y Graciela Medina (Directores), Ed. Thompson Reuters La Ley, Tomo I, Buenos Aires, 2014, p. 99.

[1112] Ibid. Confr. Art. 16, CCCN.

[1113] Los derechos, en tanto bienes, pueden ser derechos reales *per se*, e.g. Arts. 2130, 2188, 2219 y 2120 CCCN, o pueden ser objeto de otros derechos reales, sin llegar a ser derechos reales *per se* y en sí mismos, como es el caso del derecho del beneficiario y del fideicomisario en relación a un patrimonio fideicomitado.

[1114] Confr. Sebastián Balbín, *Manual de Derecho Societario*, Ed. Abeledo Perrot, tercera edición, Buenos Aires, 2018, p. 428 señala que las partes de interés son una fracción alícuota, no necesariamente iguales, en la que se divide el capital social de las sociedades de personas. La parte de interés es embargable, pero no ejecutable, debido al carácter esencial que la ley asigna al socio en este tipo de sociedades.

[1115] Esta es una opinión del autor. En contra: Maximiliano Rafael Calderón, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo V, Buenos Aires, 2016, p. 1155 quien afirma que el derecho beneficiario puede especificarse mediante criterios cuantitativos o cualitativos, tratándose de un derecho libremente cesible salvo disposición contractual en contra, incluso antes de ser aceptado. El derecho del beneficiario (y del fideicomisario) es un derecho personal y creditorio, que es susceptible de constituir el objeto de derechos reales de garantía a favor de terceros, e.g., prenda de créditos, y también es embargable por los acreedores del beneficiario, conforme al Art. 1686, CCCN.

[1116] Confr. Sebastián Balbín, *Manual de Derecho Societario...o.c.* p. 496 afirma que, si bien el Art. 226 de la Ley 19.550 dispone que las normas sobre títulos valores se aplican a las acciones, los acciones cuentan con *características propias* que las

diferencian de los títulos valores: (i) cuentan con derechos políticos; (ii) las variaciones en su valor nominal se hacen sin intervención de su titular en casos de reducción de capital; y (iii) no resulta necesaria la existencia física del título, cuando la calidad de accionista puede demostrarse mediante registros. Para Balbín, todo ello conlleva a considerar a la acción como una *figura jurídica propia*. También señala el autor citado que la Ley N° 24.587 dispuso la nominatividad de todo título valor privado emitido en el país, y limitó su forma de transmisión, no admitiéndose las acciones al portador, ni su transmisión por endoso.

Se concluye entonces que las acciones legalmente admitidas son o bien nominativas, representadas físicamente en un título –una *cosa*–; o bien, escriturales, representadas por una inscripción en una cuenta de cada acción escritural, llevada en el libro registro de accionistas –tal inscripción es un *bien*–, y su transmisión a terceros y los derechos reales que las gravan deben en éste caso notificarse a la emisora o a la sociedad que lleve el registro, e inscribirse en la cuenta pertinente.

Sostiene Balbín que la tendencia hacia la desmaterialización de las acciones escriturales se impone, y la acción escritural es una muestra de ello: “*en tal caso deben inscribirse en cuentas llevadas a nombre de sus titulares por la sociedad emisora en un registro de acciones escriturales, sujeto en lo pertinente a idénticos recaudos que los de un libro de registro de acciones, o por bancos comerciales o de inversión o cajas de valores autorizados. La calidad de accionista se presume por las constancias de las cuentas abiertas en el registro, y la sociedad es responsable ante los accionistas por los errores o irregularidades de las inscripciones, sin perjuicio de la responsabilidad del banco o caja de valores ante la sociedad, en su caso*”.

[1117]

Confr. Ignacio Alterini, *Los fundamentos del derecho real...*o.c. p. 71. Confr. Sebastián Balbín, *Manual de Derecho Societario...*o.c. p. 457 afirma que la cuota es una parte social, análoga a las partes de interés, pero con algunos caracteres propios, lo que sitúa a las cuotas sociales en una posición intermedia entre la acción y la parte de interés. Sostiene Balbín que la cuota es un bien mueble incorporeal, registrable o susceptible de publicidad registral. Así, a diferencia de las partes de interés, las cuotas sociales son partes alícuotas, son siempre cesibles, fijan el primer límite de responsabilidad de su titular y son susceptibles de embargo y venta forzada. A diferencia de las acciones, las cuotas sociales son muebles incorporales registrables, mientras que las acciones son títulos valores, y las cuotas sólo dan derecho a un voto; mientras que la acción puede otorgar hasta cinco votos por acción.

Afirma Balbín que al dividirse el capital social de la SRL en cuotas, éstas no pueden representarse en títulos, mientras que las acciones sí. Esta es una nota distintiva de las cuotas: el derecho del socio existe sin documento alguno. Su cesión requiere de un instrumento escrito, por tratarse de un acto formal, y sólo surte efecto frente a la sociedad cuando las partes interesadas entregan a la gerencia una copia de dicho instrumento, con firmas certificadas, y respecto de terceros, cuando la cesión se

inscribe en el registro público. La cesión de cuotas, afirma Balbín, es una cesión de posición contractual de acuerdo al Art. 1636, CCCN.

[1118] Confr. Ignacio Alterini, *Los fundamentos del derecho real...o.c.* p. 71.

[1119] Afirman esta relación, Renato Rabbi-Baldi Cabanillas y Ernesto Solá, en Código Civil y Comercial de la Nación Comentado...o.c. p. 93. Con relación a los derechos de las comunidades indígenas hay posiciones encontradas. Así, se sostiene, por un lado, que el mismo no sería un derecho real, sino un derecho público, en razón de su inalienabilidad e inejecutabilidad asignada por la Constitución Nacional; por otro lado, si bien se lo califica como una propiedad especial de fuente constitucional, se lo clasifica como derecho con naturaleza real. Véase ídem, p. 107.

[1120] Confr. Ignacio Alterini, *Los fundamentos del derecho real...o.c.*, p. 65.

[1121] Ibid.

[1122] Ibid.

[1123] El Poder Ejecutivo Nacional designó por Decreto N° 685/95 a los juristas: Héctor Alegría, Atilio A. Alterini, Jorge H. Alterini, Augusto César Belluscio, Antonio Boggiano, Aída Kemelmajer de Carlucci, María Josefa Méndez Costa, Julio César Rivera y Horacio Roitman para realizar un proyecto de revisión o de renovación del Código Civil Argentino. La Comisión elaboró el “*Proyecto de Código Civil de 1998 para la República Argentina*”, un proyecto de nuevo Código Civil dividido en ocho Libros, que fue elevado al Poder Ejecutivo Nacional el día 28 de diciembre de 1998. Su Art. 1816 rezaba: “*Son objeto de los derechos reales: a) Las cosas que están en el comercio. Se ejercen sobre la totalidad de ellas, o sobre una parte material, o por una alícuota. b) Los derechos en los casos previstos especialmente.*”

[1124] Confr. Ignacio Alterini, *Los fundamentos del derecho real...o.c.*, p. 68.

[1125] Idem, p. 70.

Art. 2188, CCCN: “*Especialidad en cuanto al objeto. Cosas y **derechos pueden constituir el objeto de los derechos reales de garantía.** Ese objeto debe ser actual, y estar individualizado adecuadamente en el contrato constitutivo.*” El resaltado es mío.

[1126] Idem, p. 70.

[1127] Idem, p. 71.

[1128] Idem, p. 58.

[1129] Ibid.

[1130] Ibid.

[1131] Confr. Nelson G.A. Cossari y Leandro R. N. Cossari, *Relaciones reales fácticas*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo VI, Buenos Aires, 2016, p. 153, afirman que las relaciones reales fácticas giran, principalmente, en torno al fenómeno posesorio.

En el caso de los criptoactivos, podría sostenerse que la relación de poder se ejerce y manifiesta poseyendo la llave privada que permite disponer del mismo. Aceptándose su calificación jurídica como bien mueble incorporal y registrable, los criptoactivos, en tanto bienes objeto del derecho real de dominio, o del derecho real de garantía de prenda o anticresis, requieren e implican una relación de poder, una relación real. Tal relación será la posesión –en términos del Art. 1909, CCCN– de la llave privada –i.e., corpus– en algunos casos; y también, quizás, podría ser la mera tenencia de la llave privada en otros. Piénsese, por ejemplo, en algunos contratos inteligentes sobre criptoactivos con firma privada múltiple, donde algún tenedor de una de las llaves privadas sólo la detenta en función de un acuerdo subyacente que delimita el alcance de su tenencia. Analizan los autores citados, en la p. 173, la diferencia entre posesión inmediata, y posesión mediata. Si se piensa en una llave privada de un criptoactivo, un deudor *off-chain* podría perfectamente garantizar el pago de tal deuda con una garantía *on-chain*, mediante un contrato inteligente en virtud del cual un tercero designado recibe, en garantía, la posesión de la llave privada del criptoactivo que oficia como garantía *on-chain* por el eventual repago de la deuda *off-chain*. El tercero que recibe la llave privada en garantía, es jurídicamente un sub poseedor, que presupone una relación jurídica entre el dueño del criptoactivo –poseedor superior– y el sub poseedor que posee la cosa a título de garantía a favor de un tercero designado, en virtud de lo cual está temporalmente facultado o obligado: (i) frente al deudor *off-chain*: si no cancela su deuda, entonces el subposeedor estará obligado a utilizar la llave privada para transferir el criptoactivo, en pago, al acreedor garantizado, y a la inversa, estará obligado a devolver la llave privada al deudor *off-chain* si éste cancela su deuda; y (ii) frente al acreedor *on-chain*, el tercero que recibió la llave privada en garantía estará facultado para transferir el criptoactivo si el pago no se produce *off-chain*. Este sub poseedor puede ser asimilado a un tenedor relativo desinteresado, representante del poseedor, lo que no impide que pueda percibir un emolumento por su función de tenencia.

[1132] Confr. <https://www.cftc.gov/PressRoom/PressReleases/7774-18>, recuperado el 01/05/2020.

[1133] Considera también a los criptoactivos en general como un bien inmaterial susceptible de valor: Pablo Denoya Rolla, *Las criptomonedas y naturaleza jurídica en el*

derecho comparado y Argentina, disponible al 03/05/2020 en https://bdigital.uncuyo.edu.ar/objetos_digitales/12511/4-desarrolloregional-denoyarolla-pablodaniel-unnoba.pdf. En el mismo sentido, véase Francisco Ossandón Cerda, *Tributación de las criptomonedas en Chile: desafíos regulatorios actuales*, Centro de Estudios Tributarios de la Universidad de Chile, recuperado el 16/05/2020 en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwj_9-H-o7vpAhUOHrkGHQFFBqMQFjABegQIAxAB&url=https%3A%2F%2Frevistas.uchile. [1134]

Confr. Arts. 4 y 10, Ley 22.362:

“Art. 4º — *La propiedad de una marca y la exclusividad de uso se obtienen con su registro. Para ser titular de una marca o para ejercer el derecho de oposición a su registro o a su uso se requiere un interés legítimo del solicitante o del oponente.*”

Art. — *Quien desee obtener el registro de una marca, debe presentar una solicitud que incluya nombre, domicilio real y especial electrónico según las condiciones que fije la reglamentación, la descripción de la marca y la indicación de los productos y/o servicios que va a distinguir.*”

[1135]

Confr. María Valentina Aicega, *Otras fuentes de las obligaciones (V): Teoría General de los Títulos Valores*, en *Tratado de Derecho Civil y Comercial*, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thomson Reuters La Ley, Tomo II, Buenos Aires, 2016, p. 744.

[1136]

Idem, p. 745.

[1137]

Idem, p. 746.

[1138]

“Art. 1815, CCCN.- *Concepto. Los títulos valores incorporan una obligación incondicional e irrevocable de una prestación y otorgan a cada titular un derecho autónomo, sujeto a lo previsto en el artículo 1816.*

Cuando en este Código se hace mención a bienes o cosas muebles registrables, no se comprenden los títulos valores.” El resaltado es mío.

[1139]

“Art. 1830, CCCN.- *Necesidad. Los títulos valores cartulares son necesarios para la creación, transmisión, modificación y ejercicio del derecho incorporado.*

Art. 1831, CCCN.- *Literalidad. El tenor literal del documento determina el alcance y las modalidades de los derechos y obligaciones consignadas en él, o en su hoja de prolongación.*”

[1140]

“Art. 1850, CCCN.- *Régimen. Cuando por disposición legal o cuando en el instrumento de creación se inserta una declaración expresa de voluntad de obligarse de manera incondicional e irrevocable, **aunque la prestación no se incorpore a un documento**, puede establecerse la circulación autónoma del derecho, con sujeción a lo*

dispuesto en el artículo 1820.

*La transmisión o constitución de derechos reales sobre el título valor, los gravámenes, secuestros, medidas precautorias y cualquier otra afectación de los derechos conferidos por el título valor deben efectuarse mediante **asientos en registros especiales** que debe llevar el emisor o, en nombre de éste, una caja de valores, una entidad financiera autorizada o un escribano de registro, momento a partir del cual la afectación produce efectos frente a terceros.*

A los efectos de determinar el alcance de los derechos emergentes del título valor así creado debe estarse al instrumento de creación, que debe tener fecha cierta. Si el título valor es admitido a la oferta pública es suficiente su inscripción ante la autoridad de contralor y en las bolsas o mercados en los que se negocia.

Se aplica respecto del tercero que adquiera el título valor lo dispuesto por los artículos 1816 y 1819.”

[1141]

Idem, p. 863.

[1142]

Idem, p. 866.

[1143]

Ibid.

[1144]

Ibid.

[1145]

Idem, p. 866.

[1146]

*“Art. 1820, CCCN.- Libertad de creación. Cualquier persona puede crear y emitir títulos valores en los tipos y condiciones que elija. Se comprende en esta facultad la denominación del tipo o clase de título, su forma de circulación con arreglo a las leyes generales, sus garantías, rescates, plazos, su calidad de convertible o no en otra clase de título, derechos de los terceros titulares y demás regulaciones que hacen a la configuración de los derechos de las partes interesadas, que deben expresarse con claridad y **no prestarse a confusión con el tipo, denominación y condiciones de los títulos valores especialmente previstos en la legislación vigente.***

*Sólo pueden emitirse **títulos valores abstractos** no regulados por la ley cuando se destinan a ofertas públicas, con el cumplimiento de los recaudos de la legislación específica; y también cuando los emisores son entidades financieras, de seguros o fiduciarios financieros registrados ante el organismo de contralor de los mercados de valores.”* El resaltado es mío.

[1147]

*“Art. 3° — Creación de valores negociables. Cualquier persona jurídica **puede crear y emitir valores negociables** para su negociación en mercados de los tipos y en las condiciones que elija, incluyendo los derechos conferidos a sus titulares y demás condiciones que se establezcan en el acto de emisión, **siempre que no exista confusión con el tipo, denominación y condiciones de los valores negociables previstos***

especialmente en la legislación vigente. A los efectos de determinar el alcance de los derechos emergentes del valor negociable así creado, debe estarse al instrumento de creación, acto de emisión e inscripciones registrales ante las autoridades de contralor competentes.”

[1148] Idem, p. 782.

[1149] Ibid.

[1150] Idem, p. 785.

[1151] Confr. Juan Diehl Moreno y Santiago Eraso Lomaquiz, *Criptoactivos en los mercados financieros y cambiarios*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed. CDYT, 2019, Buenos Aires, p. 186.

[1152] Idem, p. 187.

[1153] Ibid. Téngase en cuenta que el Título VIII de la Ley 27.440 reguló los instrumentos derivados, y obligó, en su Art. 189, a inscribirlos en CNV para poder producir los efectos establecidos en dicho título VIII, ser oponibles a terceros y tener fecha cierta, cuando se realizan entre contrapartes nacionales y/o extranjeras, por fuera del ámbito de negociación de mercados autorizados por la CNV. Son los llamados derivados OTC, cuyo objeto pueden perfectamente ser criptomonedas. Se volverá sobre *infra* en § 5.2.3.3.1.

[1154] Confr. Marina Bericua y Santiago Mora, *Algunas ideas sobre una eventual regulación de las ofertas iniciales de security tokens*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed. CDYT, 2019, Buenos Aires, p. 189.

[1155] Idem, p. 192.

[1156] Idem, p. 193.

[1157] Ibid.

[1158] Idem, p. 198.

[1159] Ibid.

[1160] Ibid.

[1161] Idem, p. 199.

[1162] Idem, p. 200, nota 27.

[1163] Se sigue en este apartado, en general, la exposición del autor en *El crowdfunding en Argentina: ¿Un mini-mercado de capitales simplificado?* Publicado en Temas de Derecho Comercial, Empresarial y del Consumidor, Marzo de 2018, cita on line: IUSDC285743A.

[1164] Confr. “Artículo 23, Ley 27.349.- *Definiciones. Incorpóranse al artículo 2° de la ley 26.831, las siguientes definiciones referidas al Sistema de Financiamiento Colectivo:*
Plataforma de financiamiento colectivo: son sociedades anónimas autorizadas, reguladas, fiscalizadas y controladas por la Comisión Nacional de Valores y debidamente inscriptas en el registro que al efecto se constituya, con el objeto principal de poner en contacto, de manera profesional y exclusivamente mediante portales web u otros medios análogos, a una pluralidad de personas humanas y/o jurídicas que actúan como inversores con personas humanas y/o jurídicas que solicitan financiación en calidad de emprendedores de financiamiento colectivo.

Responsable de plataforma de financiamiento colectivo: son las personas humanas designadas por los accionistas de la plataforma de financiamiento colectivo para el cumplimiento de los requerimientos exigidos por la Comisión Nacional de Valores, actuando en representación de la plataforma de financiamiento colectivo.

Emprendedor de financiamiento colectivo: es la persona humana y/o jurídica que presenta un proyecto de financiamiento colectivo con la finalidad de obtener fondos del público inversor para su desarrollo, conforme la reglamentación que a tales fines dicte la Comisión Nacional de Valores.

Proyecto de financiamiento colectivo: es el proyecto de desarrollo individualizado presentado por un emprendedor de financiamiento colectivo a través de una plataforma de financiamiento colectivo y que solicita fondos del público inversor con la finalidad de crear y/o desarrollar un bien y/o servicio.” Los resaltados son míos.

[1165] “Art. 1110, CCCN.- *Revocación. En los contratos celebrados fuera de los establecimientos comerciales y a distancia, el consumidor tiene el derecho irrenunciable de revocar la aceptación dentro de los diez días computados a partir de la celebración del contrato.*

Si la aceptación es posterior a la entrega del bien, el plazo debe comenzar a correr desde que esta última se produce.

Si el plazo vence en día inhábil, se prorroga hasta el primer día hábil siguiente.

Las cláusulas, pactos o cualquier modalidad aceptada por el consumidor durante este período que tengan por resultado la imposibilidad de ejercer el derecho de revocación se tienen por no escritos”.

[1166] Confr. Normas CNV, T.O. 2013, Título XIX, Art. 45: En el supuesto en que un Proyecto opte por efectuar sucesivas colocaciones, deberá notificar a la PFC de su intención con una antelación mínima de diez (10) días a la fecha propuesta para

iniciar la suscripción.

[1167] Confr. Normas CNV, Título XIX, Art. 46. El período de suscripción puede prorrogarse en un 20% si se produce un cambio material en el proyecto informado a los inversores antes de cumplirse el 80% del período de suscripción originariamente previsto.

[1168] Confr. Normas CNV, Título XIX, Art. 53.

[1169] Confr. Normas CNV, Título XIX, Art. 45.

[1170] Confr. Art. 12 de la Sección I, del Capítulo VI, del Título II de las Normas (T.O. 2013).

[1171] Confr. Normas CNV, Título XIX, Art. 43. La PFC deberá velar por que, en caso de adoptar la forma jurídica de una Sociedad Anónima o una Sociedad Anónima Simplificada, los socios de los Proyectos de Financiamiento Colectivo, y los miembros de sus órganos de administración y de fiscalización -titulares y suplentes-, no podrán ser:

- a) Quienes no puedan ejercer el comercio.
- b) Los condenados por los delitos previstos en los artículos 176 a 180 del Código Penal o cometidos con ánimo de lucro o contra la fe pública o que tengan pena principal, conjunta o alternativa de inhabilitación, hasta cinco (5) años después de cumplida la condena.
- c) Los fallidos y los concursados hasta cinco (5) años después de su rehabilitación.
- d) Quienes se encuentren inhabilitados por la aplicación de la sanción dispuesta en el artículo 132 inciso c) de la ley 26831 y mod.
- e) Las personas que no cumplan con los requisitos dispuestos en la normativa sobre prevención del lavado de dinero y financiación del terrorismo.

[1172] Confr. Normas CNV, Título XIX, Art. 44. En caso de emplear una SA:

- a.1) Estatuto social con sus respectivas modificaciones, si las hubiera, CUIT, sede social, página web, nómina de accionistas y composición del capital;
- a.2) Nombre de los integrantes del órgano de administración, representante legal y órgano de fiscalización, organigrama, tiempo en ejercicio, experiencia en el negocio de los últimos 3 años, o desde su constitución en caso de tener una existencia menor, y estados contables de los últimos tres años o del tiempo que llevare en operación si este fuere menor.

[1173] Confr. Normas CNV, Título XIX, Art. 44. En caso de emplear una SAS:

- b.1) Estatuto social con sus respectivas modificaciones, si las hubiera, CUIT, sede social, página web, nómina de accionistas y composición del capital;
- b.2) Nombre de los integrantes del órgano de administración, representante legal, en

su caso, órgano de fiscalización, organigrama, tiempo en ejercicio, experiencia en el negocio de los últimos 3 años, o desde su constitución en caso de tener una existencia menor, y estados contables de los últimos tres años o del tiempo que llevare en operación si este fuere menor.

[1174] Confr. Normas CNV, Título XIX, Art. 44. En caso de emplear un fideicomiso como figura para la inversión el mismo deberá constituirse de acuerdo a los términos del artículo 1666 y concordantes del Código Civil y Comercial de la Nación y deberá aportar los siguientes datos:

c.1) Denominación del fideicomiso, CUIT, contrato de constitución, patrimonio afectado en el fideicomiso;

c.2) Denominación y domicilio del fiduciario, CUIT, de corresponder nombre de los integrantes del órgano de administración del fiduciario, administradores, gerentes, organigrama, tiempo en ejercicio, experiencia en el negocio de los últimos 3 años, o desde su constitución en caso de tener una existencia menor, y estados contables de los últimos tres años o del tiempo que llevare en operación si este fuere menor;

c.3) Identificación y domicilio de los fiduciantes y de los beneficiarios.

[1175] Confr. Normas CNV, Título XIX, Art. 47.

[1176] La información debe presentarse dentro del plazo de setenta (70) días corridos de cerrado el ejercicio, o dentro de los dos (2) días de su aprobación por el órgano de administración, lo que ocurra primero, y por lo menos veinte (20) días corridos antes de la fecha para la cual ha sido convocada la Asamblea de Accionistas que la considerará.

[1177] Las Normas de la CNV, Título XIX, Art. 49, inc. d) hacen referencia a una Comisión Fiscalizadora. Entendemos que sólo será exigible la conformación de Comisión Fiscalizadora cuando el vehículo constituido (o a ser constituido) por el Emprendedor de Financiamiento Colectivo obtenga capitalización que supere los Cincuenta Millones de Pesos (confr. Ley N° 19.550, Art. 299, inc. 2).

[1178] Confr. Reuters, *U.S. crowdfunding offers new capital source, SEC finds*, recuperado el 01/05/2020 en <https://www.reuters.com/article/us-usa-sec-crowdfunding/u-s-crowdfunding-offers-new-capital-source-sec-finds-idUSKBN1672FE>.

[1179] Por caso, la SEC reglamentó un techo que tiene el doble de altura del reglamentado por CNV (USD 2.200 vs. AR\$ 20.000) y que además no toma la menor de las variables, sino la mayor: si los ingresos anuales o el valor neto de los activos es menor a USD 107.000, durante un período de 12 meses, entonces se permite invertir *el mayor de los importes* entre (i) USD 2.200 o (ii) el importe que equivalga al 5% de los

ingresos anuales o el 5% del valor neto de los activos del inversor, de éstos considerándose el menor. Confr. https://www.sec.gov/oiea/investor-alerts-bulletins/ib_crowdfunding-.html recuperado el 01/05/2020.

[1180]

Por ejemplo, podría establecerse como techo “alternativo” para este tipo de micro-inversión el importe equivalente a 4 salarios mínimos, vitales y móviles, o el 5% de la suscripción de un Proyecto de Financiamiento Colectivo, el que resulte mayor.

[1181]

Véase *supra* en § 3.3.1.2.

[1182]

Los requisitos para la emisión de valores negociables por PyMES están contenidos en las Normas de la CNV (T.O. 2013), Título II, Capítulo VI, en tres Secciones. Estas emisiones PyMES están exentas del pago de tasas de fiscalización y control, de constituir comité de auditoría, y sólo deben tener una sindicatura individual.

Los montos máximos de emisión pueden ascender a los 500 Millones de Pesos y sólo pueden ser adquiridos por inversores calificados: 1) El Estado Nacional, las Provincias y Municipalidades, Entidades Autárquicas, Sociedades del Estado y Empresas del Estado, 2) Organismos Internacionales y Personas Jurídicas de Derecho Público, 3) Fondos Fiduciarios Públicos, 4) La Administración Nacional de la Seguridad Social (ANSeS) – Fondo de Garantía de Sustentabilidad (FGS), 5) Cajas Previsionales, 6) Bancos y Entidades Financieras Públicas y Privadas, 7) Fondos Comunes de Inversión, 8) Fideicomisos Financieros con oferta pública, 9) Compañías de Seguros, de Reaseguros y Aseguradoras de Riesgos de Trabajo, 10) Sociedades de Garantía Recíproca, 11) Personas Jurídicas registradas por la CNV como agentes, cuando actúen por cuenta, 12) Personas humanas o jurídicas, distintas de las enunciadas en los incisos anteriores, que al momento de efectuar la inversión cuenten con inversiones en valores negociables y/o depósitos en entidades financieras por un monto equivalente a UNIDADES DE VALOR ADQUISITIVO TRESCIENTAS CINCUENTA MIL (UVA 350.000), y 13) **Personas jurídicas constituidas en el extranjero y personas humanas con domicilio real en el extranjero**. Existen modelos de prospectos simplificados para estas emisiones.

[1183]

Confr. Marina Bericua y Santiago Mora, *Algunas ideas sobre una eventual regulación de las ofertas iniciales de security tokens...* o.c. p. 200.

[1184]

Confr. Julián Dunayevich y Daniel Franca, *Blockchain Federal Argentina: una plataforma multiservicios basada en el modelo de gobernanza multisectorial*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed. CDYT, 2019, Buenos Aires, p. 213.

Afirman los autores citados que BFA toma el software de Ethereum. Siguiendo esta base, todos los desarrollos y las modificaciones que se realicen serán igualmente

abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes de la organización. De esta forma, la transparencia inherente en el modelo queda también garantizada desde el código.

[1185] Idem, p. 201.

[1186] Idem, p. 210.

[1187] Idem, p. 212. Afirman los autores citados que se trata de *“una blockchain que funciona de forma permitida bajo un consenso basado en prueba de autoridad: la red se estructura sobre la base de un conjunto confiable, una determinada cantidad de nodos selladores a partir del consenso de las partes que integran BFA y respaldados por la infraestructura de las instituciones, empresas u organismos responsables de cada uno de ellos. Así, el procesamiento no se basa en un conjunto de mineros anónimos compitiendo por la creación de un bloque sino en la cooperación entre aquellos que representan a distintos sectores.”*

[1188] Ibid. Afirman Dunayevich y Franca, o.c., p. 212, que BFA *“no posee criptomoneda asociada. El incentivo para participar en BFA es favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores. Dado esto, no es necesaria la implementación de una moneda virtual para aprovechar las ventajas que proporciona Blockchain. Cuando el objetivo de participar y fortalecer la iniciativa no es la acumulación de criptomonedas, aparece un camino caracterizado por la colaboración en lugar de la competencia.”*

[1189] Idem, p. 211.

[1190] Afirman Dunayevich y Franca, o.c., p. 212 que *“Al no depender del minado de criptomonedas y del esfuerzo por obtener una recompensa, no se hace necesario contar con gran cantidad de computadoras a disposición de la resolución de algoritmos complejos, con el gasto de energía que eso conlleva. Por ello se habilita la implementación de mecanismos de consenso eficientes, tanto en lo relativo a cantidad de transacciones por unidad de tiempo como en el consumo eléctrico. En este sentido, BFA necesita de muchos menos recursos que una blockchain tradicional basada en prueba de trabajo.”*

[1191] Ibid.

[1192] Idem, p. 213. Puntualizan los autores citados que todas las transacciones realizadas sobre Blockchain Federal Argentina no tienen costo. Al no poseer una criptomoneda asociada, y al estructurar la red bajo el modelo de prueba de autoridad con un costo de infraestructura marginal, las transacciones son gratuitas. El

“combustible” necesario es *Ether*, que BFA distribuye a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma. El *Ether* no tiene ningún tipo de valor económico y se envía periódicamente mediante una interfaz operada por la organización, será provisto sin costo alguno por BFA, quien también será responsable de tomar las medidas necesarias para evitar abusos. Señalan los autores, en la nota p. 213, nota 8, que la *destilería* es el mecanismo mediante el cual se distribuye *Ether* a todos los nodos de BFA que lo necesiten. Permite implementar un modelo donde se evita la especulación y/o el tráfico, además de posibilitar métodos para detectar el abuso. [1192]

[1193] Ibid.

[1194] Idem, p. 214

[1195] Véase *infra*, en § 3.5.1.10.1.

[1196] Ibid.

[1197] Véase *supra*, en § 3.4.5.1.

[1198] Confr. Santiago Mora, *La tecnología blockchain: contratos inteligentes, ofertas iniciales de monedas y demás casos de uso...o.c.*, p. 133, y doctrina citada por Mora en nota 57.

[1199] Confr. “Art. 286, CCCN.- *Expresión escrita. La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos.*” El resaltado es mío.

[1200] Confr. “Art. 287, CCCN.- *Instrumentos privados y particulares no firmados. Los instrumentos particulares pueden estar firmados o no. Si lo están, se llaman instrumentos privados.*

Si no lo están, se los denomina instrumentos particulares no firmados; esta categoría comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información.” El resaltado es mío.

[1201] Confr. “Art. 288, CCCN.- *Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo.*

En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitadamente la autoría e integridad del instrumento.” El resaltado es mío.

[1202] Confr. “Art. 319, CCCN.- Valor probatorio. El valor probatorio de los instrumentos particulares debe ser apreciado por el juez ponderando, entre otras pautas, la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y **la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen.**” El resaltado es mío.

[1203] Confr. “Art. 1106, CCCN.- Utilización de medios electrónicos. Siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un **soporte electrónico u otra tecnología similar.**”

[1204] Confr. “Art. 1107, CCCN.- Información sobre los medios electrónicos. Si las partes se valen de técnicas de comunicación electrónica o similares para la celebración de un contrato de consumo a distancia, el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, **todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos.**” El resaltado es mío.

[1205] Confr. “Art. 1109, CCCN.- Lugar de cumplimiento. En los contratos celebrados fuera de los establecimientos comerciales, a distancia, y con utilización de medios electrónicos o similares, se considera lugar de cumplimiento aquel en el que el consumidor recibió o debió recibir la prestación. Ese lugar fija la jurisdicción aplicable a los conflictos derivados del contrato. La cláusula de prórroga de jurisdicción se tiene por no escrita.”

[1206] Confr. “Art. 1110, CCCN.- Revocación. En los contratos celebrados fuera de los establecimientos comerciales y a distancia, el consumidor tiene el derecho irrenunciable de revocar la aceptación dentro de los diez días computados a partir de la celebración del contrato. Si la aceptación es posterior a la entrega del bien, el plazo debe comenzar a correr desde que esta última se produce. Si el plazo vence en día inhábil, se prorroga hasta el primer día hábil siguiente. Las cláusulas, pactos o cualquier modalidad aceptada por el consumidor durante este período que tengan por resultado la imposibilidad de ejercer el derecho de revocación se tienen por no escritos.”

[1207] Confr. “Art. 1120, CCCN.- Situación jurídica abusiva. Se considera que existe una situación jurídica abusiva cuando el mismo resultado se alcanza a través de la predisposición de una pluralidad de actos jurídicos conexos.”

[1208] Confr. Andrés Chomczyk, *Contratos inteligentes o software obediente*, en Santiago Mora y Pablo Palazzi (compiladores), *Fintech: Aspectos Legales*, Tomo II, Ed.

CDYT, 2019, Buenos Aires, p. 154.

[\[1209\]](#)

Idem, p. 155.

[\[1210\]](#)

Ibid.

[\[1211\]](#)

Idem, p. 156.

[\[1212\]](#)

Idem, p. 158.

[\[1213\]](#)

Idem, p. 159.

[\[1214\]](#)

Ibid.

[\[1215\]](#)

La regulación de esta forma de expresión del consentimiento está contenida en los Arts. 984 a 989, CCCN.

[\[1216\]](#)

Confr. Fulvio G. Santarelli, *Contratos Autoejecutables: “Smart Contracts”*: *Apenas una descripción para proponer su uso virtuoso*, publicado en Diario La Ley, El presente tecnológico de la profesión legal, 03/06/2020, p. 14.

[\[1217\]](#)

Ibid.

[\[1218\]](#)

Confr. Andrés Sánchez Herrero, *Contratos celebrados por adhesión a cláusulas generales predispuestas*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo IV, Buenos Aires, 2016, p. 187.

[\[1219\]](#)

Idem, p. 188.

[\[1220\]](#)

Idem, p. 189.

[\[1221\]](#)

Ibid.

[\[1222\]](#)

Idem, p. 190.

[\[1223\]](#)

Idem, p. 193.

[\[1224\]](#)

Idem, p. 196.

[\[1225\]](#)

Idem, p. 197.

[\[1226\]](#)

Idem, p. 205.

[\[1227\]](#)

Ibid.

[\[1228\]](#)

Idem, p. 207.

[1229]

Idem, p. 214.

[1230]

Idem, p. 219.

[1231]

Idem, p. 222. “Art. 1119, CCCN.- Regla general. Sin perjuicio de lo dispuesto en las leyes especiales, es abusiva la cláusula que, habiendo sido o no negociada individualmente, tiene por objeto o por efecto provocar un desequilibrio significativo entre los derechos y las obligaciones de las partes, en perjuicio del consumidor.”

[1232]

Idem, p. 224.

[1233]

Ibid.

[1234]

Idem, p. 225.

[1235]

Idem, p. 226.

[1236]

Idem, p. 227.

[1237]

Confr. Andrés Chomczyk, *Contratos inteligentes o software obediente...o.c.* p. 161.

[1238]

Idem, p. 162.

[1239]

El autor quiere agradecer especialmente al Mag. Martín Bertoni por su colaboración en este apartado.

[1240]

Confr. <https://www.ifrs.org/-/media/feature/meetings/2018/november/iasb/ap12d-cryptocurrencies.pdf>, disponible al 02/05/2020.

[1241]

Confr. <https://www.ifrs.org/projects/2019/holdings-of-cryptocurrencies/>, recuperado el 02/05/2020. Véase también el estudio de KPMG preparado por Jonathan Dingli, *accounting for cryptoassets*, recuperado el 02/05/2020 en <https://home.kpmg/mt/en/home/insights/2019/12/accounting-for-cryptoassets.html>, y el informe *Accounting for cryptoassets: from a Holder's perspective*, elaborado por la Institute of Singapore Chartered Accountants, recuperado el 02/05/2020 en <https://isca.org.sg/media/2823668/ed-frg-2-accounting-for-cryptoassets-from-a-holder-s-perspective.pdf>.

[1242]

Confr. <https://www.ifrs.org/news-and-events/updates/ifric-updates/june-2019/#8>, recuperado el 02/06/2020. Se sostuvo como justificación que: “Some cryptocurrencies can be used in exchange for particular good or services. However, **the Committee noted that it is not aware of any cryptocurrency that is used as a medium**

of exchange and as the monetary unit in pricing goods or services to such an extent that it would be the basis on which all transactions are measured and recognised in financial statements. Consequently, the Committee concluded that a holding of cryptocurrency is not cash because cryptocurrencies do not currently have the characteristics of cash.” El resaltado es mío.

Se considera que a la misma conclusión se puede arribar mediante la lectura transversal de la NIC 32 y la NIIF 9, con foco en la NIC 32 que tipifica el concepto de Activo y Pasivo financiero. Véase <http://www.facpce.org.ar:8080/miniportal/archivos/nic/NIC32.pdf>, disponible al 02/05/2020.

Se puede llegar a la conclusión de que las criptomonedas pueden serlo o no serlo, dependiendo si las mismas están “respaldadas” por un activo que resulte ser Financiero o no. Dependerá del análisis fino de cada criptoactivo poder conceptualizarlos como “instrumentos financieros”.

Así, una criptomoneda estable respaldada en U\$D cumplirá con todas las definiciones dadas de NIC 32 para ser tipificada como Activo Financiero y, por ello, su tenedor debería darle tratamiento de acuerdo a NIIF 9, puesto que cumple con la caracterización de activo Financiero. En el caso de Bitcoin, no es una criptomoneda estable, al no estar respaldada por ningún tipo de activo, pero cumple con la condición de activo financiero, de acuerdo a lo previsto en NIC 32, pero no tipifica como “Efectivo”, sino que tipifica como Activo Financiero, concepto significativamente diferente. No es efectivo, ni es equivalente a Efectivo, dado su exposición a cambios significativos de Valor (elevada volatilidad). En el caso de un token respaldado por un activo real (e.g. una botella de vino), a pesar de poder operarse en un *Exchange*, el token no tipifica como Activo Financiero de acuerdo a NIC 32, por lo tanto no es un activo financiero; pero podría ser un Inventario (Bien de Cambio) si el emisor en el devenir ordinario de su negocio (operatoria natural) compra y vende bebidas. Caso contrario podría tipificar como “Activo Intangible”.

[1243]

Ampliar en <https://www.ifrs.org/issued-standards/list-of-standards/ias-2-inventories/>, recuperado el 02/05/2020. Se afirma que “*IAS 2 provides guidance for determining the cost of inventories and the subsequent recognition of the cost as an expense, including any write-down to net realisable value. It also provides guidance on the cost formulas that are used to assign costs to inventories. Inventories are measured at the lower of cost and net realisable value. Net realisable value is the estimated selling price in the ordinary course of business less the estimated costs of completion and the estimated costs necessary to make the sale. The cost of inventories includes all costs of purchase, costs of conversion (direct labour and production overhead) and other costs incurred in bringing the inventories to their present location and condition. The cost of inventories is assigned by: (i) specific identification of cost for items of inventory that are not ordinarily interchangeable; and (ii) the first-in, first-out*

or weighted average cost formula for items that are ordinarily interchangeable (generally large quantities of individually insignificant items). When inventories are sold, the carrying amount of those inventories is recognised as an expense in the period in which the related revenue is recognised. The amount of any write-down of inventories to net realisable value and all losses of inventories are recognised as an expense in the period the write-down or loss occurs.” El resaltado es mío.

Ahora bien, el encuadramiento de un criptoactivo como un bien de cambio (activo corriente) o un activo intangible (activo fijo) dependerá de que el destino del criptoactivo de que se trate se corresponda (o no) con las actividades “normales el curso del negocio de la entidad”, ya que los inventarios son activos: (i) poseídos para ser vendidos en el curso normal de operaciones; (ii) en proceso de producción con vista a esa venta o (iii) en forma de materiales o suministros que serán consumidos en el proceso de producción o en la prestación de servicios.

[1244]

Ampliar en <https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/> recuperado al 02/05/2020. Se afirma que “**IAS 38 sets out the criteria for recognising and measuring intangible assets and requires disclosures about them. An intangible asset is an identifiable non-monetary asset without physical substance. Such an asset is identifiable when it is separable, or when it arises from contractual or other legal rights. Separable assets can be sold, transferred, licensed, etc. Examples of intangible assets include computer software, licences, trademarks, patents, films, copyrights and import quotas. Goodwill acquired in a business combination is accounted for in accordance with IFRS 3 and is outside the scope of IAS 38. Internally generated goodwill is within the scope of IAS 38 but is not recognised as an asset because it is not an identifiable resource. Expenditure for an intangible item is recognised as an expense, unless the item meets the definition of an intangible asset, and: (i) it is probable that there will be future economic benefits from the asset; and (ii) the cost of the asset can be reliably measured. The cost of generating an intangible asset internally is often difficult to distinguish from the cost of maintaining or enhancing the entity’s operations or goodwill. For this reason, internally generated brands, mastheads, publishing titles, customer lists and similar items are not recognised as intangible assets. The costs of generating other internally generated intangible assets are classified into whether they arise in a research phase or a development phase. Research expenditure is recognised as an expense. Development expenditure that meets specified criteria is recognised as the cost of an intangible asset. Intangible assets are measured initially at cost. After initial recognition, an entity usually measures an intangible asset at cost less accumulated amortisation. It may choose to measure the asset at fair value in rare cases when fair value can be determined by reference to an active market. An intangible asset with a finite useful life is amortised and is subject to impairment testing. An intangible asset with an indefinite useful life is not amortised, but is tested annually for impairment. When an intangible asset is disposed of, the**

gain or loss on disposal is included in profit or loss.”El resaltado es mío.

Evidentemente, si el criptoactivo en los términos de creación estipulados en el White Paper tiene otra naturaleza económica y jurídica, porque, por ejemplo, tiene reconocida y vinculada una deuda, una obligación exigible al emisor de entregar un bien o un servicio, entonces quizás su encuadre contable no será en el activo, sino en el pasivo corriente, o no corriente.

[1245]

Confr.

[https://www.ifrs.org/-](https://www.ifrs.org/-/media/feature/meetings/2018/september/ifric/ap04c.pdf)

[/media/feature/meetings/2018/september/ifric/ap04c.pdf](https://www.ifrs.org/-/media/feature/meetings/2018/september/ifric/ap04c.pdf), recuperado al 02/05/2020.

[1246]

Idem, párrafo 9.

[1247]

Ibid.

[1248]

Idem, párrafo 27. Se afirma que *“IFRS 15 applies to all contracts with customers except contracts within the scope of other IFRS Standards and non-monetary exchanges between entities in the same line of business to facilitate sales to customers or potential customers. A contract is defined in paragraph 10 of IFRS 15 as an **agreement between two or more parties that creates enforceable rights and obligations.** Paragraph 6 of IFRS 15 defines a customer as a party that has contracted with an entity to obtain goods or services that are an output of the entity’s ordinary activities in exchange for consideration.”* Los resaltados son míos.

En efecto, un TGE puede no necesariamente implicar un ingreso por venta, sino también un pasivo en especie, aunque lo normal y habitual será que un TGE sea un contrato con clientes y permita reconocer ingresos por ventas.

[1249]

Idem, párrafo 16.

[1250]

Idem, párrafo 18. En puridad, si la venta de tokens genera un ingreso por ventas, impacta tanto en el activo y como en el Patrimonio Neto, dado que el reconocimiento de Ingresos implica también un impacto en éste vía reconocimient de Resultados del Período.

[1251]

Idem, párrafo 25. Se precisa que: *“IAS 37 applies to all provisions and contingent liabilities, except those resulting from executory contracts and those covered by another IFRS Standard. Paragraph 10 of IAS 37 defines a **provision as ‘a liability of uncertain timing or amount’ and a contingent liability as: (a) a possible obligation that arises from past events and whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the entity; or (b) a present obligation that arises from past events but is not recognised because:***

(i) it is not probable that an outflow of resources embodying economic benefits will be required to settle the obligation; or (ii) the amount of the obligation cannot be measured

with sufficient reliability.”

El pasivo a reconocer no sería contingente. Solo sería contingente cualquier evento oneroso que implique pérdidas potenciales de forma accesoria al evento principal cuyo desenlace dependa de un evento aleatorio futuro. En términos generales esta emisión tiene tratamiento vía IFRS 15, siendo primariamente un *anticipo* cobrado por un contrato con un cliente.

[1252]

Confr. <https://www.ifrs.org/issued-standards/list-of-standards/ias-32-financial-instruments-presentation/>, recuperado al 02/05/2020. Se afirma que *“IAS 32 specifies presentation for financial instruments. The recognition and measurement and the disclosure of financial instruments are the subjects of IFRS 9 or IAS 39 and IFRS 7 respectively. **For presentation, financial instruments are classified into financial assets, financial liabilities and equity instruments.** Differentiation between a financial liability and equity depends on whether an entity has an obligation to deliver cash (or some other financial asset). However, exceptions apply. When a transaction will be settled in the issuer’s own shares, classification depends on whether the number of shares to be issued is fixed or variable.*

***A compound financial instrument, such as a convertible bond, is split into equity and liability components.** When the instrument is issued, the equity component is measured as the difference between the fair value of the compound instrument and the fair value of the liability component. Financial assets and financial liabilities are offset only when the entity has a legally enforceable right to set off the recognised amounts, and intends either to settle on a net basis or to realise the asset and settle the liability simultaneously.”* Los resaltados son míos.

[1253]

En este sentido se pronuncian Christos Kinanis, Demetra Constantinou, Nikoss Athanasiou y Antonia Hadjiantoniou, en *Security token offerings: equity or debt? How financial statements are affected*, disponible al 02/05/2020 en <https://www.legal500.com/developments/thought-leadership/security-token-offerings-equity-or-debt-how-financial-statements-are-affected/>.

[1254]

Idem. Afirman los autores citados que si el token es asimilable a equity, entonces: *“According to the guidance given by IFRS 9, on the initial recognition of financial instruments, **the instruments are measured at fair value.** The fair value at initial recognition is normally the transaction price. Therefore, **the amount of funds raised from the investors during the STO represents the initial fair value.***

*Since the tokens are classified as equity instruments, **the issuing company needs to recognize the tokens in the equity and reserves of the issuing company.** As far as the subsequent measurement is concerned, the tokens will not be revalued at each year end, being classified as equity instrument.”* El resaltado es mío.

[1255] Confr. <https://www.ifrs.org/issued-standards/list-of-standards/ias-32-financial-instruments-presentation/>, párrafo 21.

[1256] Confr. Christos Kinanis, Demetra Constantinou, Nikoss Athanasiou y Antonia Hadjiantoniou, en *Security token offerings...o.c.*, afirman que si el security token es deuda: ***“According to the guidance given by IFRS 9, on the initial recognition of financial instruments, an entity recognises a financial liability in its statement of financial position, when a contractual obligation arises. The initial recognition will be at fair value, which represent the funds raised from the investors.***

Regarding the subsequent measurement, according to the standard, financial liabilities can be measured at either (i) Amortised cost using the effective interest method or (ii) Fair Value through profit or loss

It is worth noting that the choice of the appropriate measurement method will depend on the specific characteristics and promises stated during the issue of the tokens and the published white paper.

In the case that the token will be redeemed back at its original value, and the tokens will generate a fixed return to the investors, then the Amortised Cost method would be the most appropriate method.

In the absence of the above characteristics, the Fair Value method (i.e. the expecting value of the obligation to be settled) may be the most appropriate method for subsequent measurement. Any unrealised increase/decrease of the fair value of the liability, will be recorded under other comprehensive income of the issuing company.” El resultado es mío.

[1257] Idem, párrafo 23. Los pasivos financieros –*financial liabilities*– son aquellos que tienen base contractual y obligan ***“(1) to deliver cash or another financial asset to another entity; or (2) to exchange financial assets or financial liabilities with another entity under conditions that are potentially unfavourable to the entity; or (3) a contract that will or may be settled in the entity’s own equity instruments and is: (i) a non-derivative for which the entity is or may be obliged to deliver a variable number of the entity’s own equity instruments; or (ii) a derivative that will or may be settled other than by the exchange of a fixed amount of cash or another financial asset for a fixed number of the entity’s own equity instruments. For this purpose, rights, options or warrants to acquire a fixed number of the entity’s own equity instruments for a fixed amount of any currency are equity instruments if the entity offers the rights, options or warrants pro rata to all of its existing owners of the same class of its own non-derivative equity instruments. Also, for these purposes the entity’s own equity instruments do not include puttable financial instruments that are classified as equity instruments in accordance with paragraphs 16A and 16B, instruments that impose on the entity an obligation to deliver to another party a pro rata share of the net assets of the entity only on liquidation and are classified as equity instruments in accordance with paragraphs 16C***

and 16D, or instruments that are contracts for the future receipt or delivery of the entity's own equity instruments.”

[1258]

Confr. Christos Kinanis, Demetra Constantinou, Nikoss Athanasiou y Antonia Hadjiantoniou, en *Security token offerings: equity..o.c.* aclaran el punto en estos términos: “*the prominent feature of debt instruments is that **the issuer does not have the unconditional right to avoid delivering cash or another financial asset to settle a contractual obligation.** Other factors that may indicate the existence of a debt instrument are the following: (i) Any variability in either the number of own equity shares delivered or in the amount of cash/financial assets received; (ii) Limited life to the instrument; (iii) Redemption is at the option of the instrument holder; (iv) **Redemption is triggered by a future uncertain event which is beyond the control of both the holder and issuer of the instrument,** and (v) Dividends (returns) are non-discretionary but mandatory”*

[1259]

Ibid. Afirman: “*it is worth mentioning that a security token may have both the characteristics of debt and equity instrument, consequently, the classification may prove to be a challenging process. In such case, in our opinion, **the characteristics of the tokens should be weighed against that of debt and equity instruments, and the classification should be made accordingly.***” El resaltado es mío.

[1260]

Confr. Carlos Eduardo Tambussi y María Fernanda Yapur, *Régimen de Defensa del Consumidor (I) Introducción*, en *Tratado de Derecho Civil y Comercial*, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo II, Buenos Aires, 2016, p. 891.

[1261]

Idem, p. 893.

[1262]

Idem, p. 895.

[1263]

Idem, p. 897.

[1264]

Confr. Tatiana Cutts, *Smart Contrats and Consumers*, publicado en *West Virginia Law Review*, Vol. 122, número 2, 2019, disponible al 03/05/2020 en <https://researchrepository.wvu.edu/cgi/viewcontent.cgi?article=5358&context=vwlr>, p. 436.

[1265]

Idem, p. 439.

[1266]

Idem, p. 442.

[1267]

Confr., Laurence Ingle, *Smart contracts and consumer law: does New Zealand need to wise up?* Recuperado el 03/05/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3466523, p.

[1268] Reguladas en el Art. 36 de la Ley 24.240.

[1269] Confr., Laurence Ingle, *Smart contracts and consumer law...o.c.*, p. 14.

[1270] Disponible al 03/05/2020 en <http://www.legislation.govt.nz/act/public/2003/0052/latest/DLM211512.html>

[1271] Confr. <http://www.legislation.govt.nz/act/public/2003/0052/latest/DLM6501355.html>, recuperado el 03/05/2020.

[1272] Confr., Laurence Ingle, *Smart contracts and consumer law...o.c.*, p. 19.

[1273] Confr. Art. 42, CN: “Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección y a condiciones de trato equitativo y digno. Las autoridades proveerán a la protección de esos derechos, a la educación para el consumo, a la defensa de la competencia contra toda forma de distorsión de los mercados, al control de los monopolios naturales y legales, al de la calidad y eficiencia de los servicios públicos, y a la constitución de asociaciones de consumidores y de usuarios. La legislación establecerá procedimientos eficaces para la prevención y solución de conflictos, y los marcos regulatorios de los servicios públicos de competencia nacional, previendo la necesaria participación de las asociaciones de consumidores y usuarios y de las provincias interesadas, en los organismos de control.”

[1274] Confr. Código Civil y Comercial de la Nación, Libro III, Título III, *Contratos de consumo*, *Contratos de consumo*, incluyendo una regulación específica de los contratos bancarios para los consumidores en el Título IV, *Contratos en particular*, Capítulo 12, *contratos bancarios*.

[1275] La Ley de Defensa del Consumidor N° 24.240 fue publicada en el Boletín Oficial el 15/10/1993, y fue modificada por las leyes 24.568, 24.787, 24.806, 24.999, 26.361, 26.993, 26.994, 27.250, 27.265, 27.266, 27.521 y 27.545.

[1276] Confr. Art. 1092, CCCN. “Relación de consumo. Consumidor. Relación de consumo es el vínculo jurídico entre un proveedor y un consumidor. Se considera consumidor a la persona humana o jurídica que adquiere o utiliza, en forma gratuita u onerosa, bienes o servicios como destinatario final, en beneficio propio o de su grupo familiar o social.

Queda equiparado al consumidor quien, sin ser parte de una relación de consumo como consecuencia o en ocasión de ella, adquiere o utiliza bienes o servicios, en forma gratuita u onerosa, como destinatario final, en beneficio propio o de su grupo familiar

o social.”

[1277]

Confr. Art. 1, Ley N° 24.240: “Objeto. Consumidor. Equiparación. La presente ley tiene por objeto la defensa del consumidor o usuario. Se considera consumidor a la persona física o jurídica que adquiere o utiliza, en forma gratuita u onerosa, bienes o servicios como destinatario final, en beneficio propio o de su grupo familiar o social. Queda equiparado al consumidor quien, sin ser parte de una relación de consumo como consecuencia o en ocasión de ella, adquiere o utiliza bienes o servicios, en forma gratuita u onerosa, como destinatario final, en beneficio propio o de su grupo familiar o social.”

[1278]

Confr. Carlos Eduardo Tambussi y María Fernanda Yapur, *Régimen de Defensa del Consumidor (I) Introducción...o.c.*, p. 921 se refiere a los usuarios indirectos como aquellos que no participan de la relación de consumo, pero como consecuencia o en ocasión de ella, adquieren o utilizan bienes, servicios o contratos inteligentes, por integrar el grupo familiar o social del usuario directo.

[1279]

Idem, p. 919. Se señala que al incluir a la persona jurídica como consumidora o usuaria, Argentina no ha seguido el criterio europeo. La inclusión de la persona jurídica, sin embargo, quedará condicionada a que la persona jurídica no integre o utilice un contrato inteligente como insumo directo de o en otros bienes o servicios a ser comercializados. Señala Tambussi que el presupuesto de debilidad de la persona jurídica que contrata con un experto es lo que habilita su protección consumeril, en tanto se verifique la situación de verdadera inferioridad. La carga de la prueba de la no incorporación a un proceso productivo corre por cuenta de quien alegue no haber tratado con un consumidor.

[1280]

Ibid.

[1281]

Confr. Art. 1093, CCCN.- “Contrato de consumo. Contrato de consumo es el celebrado entre un consumidor o usuario final con una persona humana o jurídica que actúe profesional u ocasionalmente o con una empresa productora de bienes o prestadora de servicios, pública o privada, que tenga por objeto la adquisición, uso o goce de los bienes o servicios por parte de los consumidores o usuarios, para su uso privado, familiar o social.”

[1282]

Confr. Art. 2, Ley N° 24.240: “Proveedor. Es la persona física o jurídica de naturaleza pública o privada, que desarrolla de manera profesional, aun ocasionalmente, actividades de producción, montaje, creación, construcción, transformación, importación, concesión de marca, distribución y comercialización de bienes y servicios, destinados a consumidores o usuarios. Todo proveedor está obligado al cumplimiento de la presente ley.

No están comprendidos en esta ley los servicios de profesionales liberales que

requieran para su ejercicio título universitario y matrícula otorgada por colegios profesionales reconocidos oficialmente o autoridad facultada para ello, pero sí la publicidad que se haga de su ofrecimiento. Ante la presentación de denuncias, que no se vincularen con la publicidad de los servicios, presentadas por los usuarios y consumidores, la autoridad de aplicación de esta ley informará al denunciante sobre el ente que controle la respectiva matrícula a los efectos de su tramitación.”

[1283]

Confr. Carlos Eduardo Tambussi y María Fernanda Yapur, *Régimen de Defensa del Consumidor (I) Introducción...o.c.*, p. 929 señalan que la única exclusión legal del concepto de proveedor son las profesiones liberales, que ofrecen servicios por cuenta propia y autónoma, y que están sujetos a normas específicas de conducta por parte de colegios profesionales, entidades de derecho público no estatal, que detentan por delegación del Estado el control disciplinario de la matrícula de sus colegiados. En éstos casos excluidos, igualmente la publicidad de servicios profesionales cae dentro del régimen del consumo.

[1284]

Art. 1100, CCCN.- “Información. El proveedor está obligado a suministrar información al consumidor en forma cierta y detallada, **respecto de todo lo relacionado con las características esenciales de los bienes y servicios que provee, las condiciones de su comercialización y toda otra circunstancia relevante para el contrato**. La información debe ser siempre gratuita para el consumidor y proporcionada con la claridad necesaria que permita su comprensión.” El resaltado es mío.

[1285]

Art. 4, Ley N° 24.240.- “Información. El proveedor está obligado a suministrar al consumidor en forma cierta, clara y detallada todo lo relacionado con las características esenciales de los bienes y servicios que provee, y las condiciones de su comercialización. La información debe ser siempre gratuita para el consumidor y proporcionada en soporte físico, con claridad necesaria que permita su comprensión. Solo se podrá suplantar la comunicación en soporte físico si el consumidor o usuario optase de forma expresa por utilizar cualquier otro medio alternativo de comunicación que el proveedor ponga a disposición.”

[1286]

Sin embargo, puede afirmarse que el proveedor de contratos inteligentes, o que utiliza contratos inteligentes para comercializar otro tipo de bienes y servicios, debiera poder demostrar que el usuario con el que contrató mediante un smart contract no es un profano –si tal fuera efectivamente el caso–, lo que sería posible, por ejemplo, si el usuario conociera lenguajes de programación en general, y en particular, el lenguaje con el cual se haya programado el contrato inteligente que genera el conflicto de consumo. Este criterio es equitativo, al basarse en las circunstancias específicas que anteceden y rodean al uso de smart contracts con destino final. En alguna medida, un criterio similar al propuesto se aplica en materia de vicios ocultos, confr. Art. 1053,

CCCN, cuando se libera al transmitente por los defectos del bien que el adquirente pudo haber conocido mediante un examen adecuado, si el adquirente –usuario del contrato inteligente– razonablemente pudo haber detectado tal defecto de programación, en función de su preparación científica o técnica previa.

[1287]

Confr. Carlos Eduardo Tambussi y María Fernanda Yapur, *Régimen de Defensa del Consumidor (I) Introducción...o.c.*, p. 973.

[1288]

Confr. Art. 37, Ley N° 24.240: “Interpretación. Sin perjuicio de la validez del contrato, se tendrán por no convenidas: a) Las cláusulas que desnaturalicen las obligaciones o limiten la responsabilidad por daños; b) Las cláusulas que importen renuncia o restricción de los derechos del consumidor o amplíen los derechos de la otra parte; c) Las cláusulas que contengan cualquier precepto que imponga la inversión de la carga de la prueba en perjuicio del consumidor.

La interpretación del contrato se hará en el sentido más favorable para el consumidor. Cuando existan dudas sobre los alcances de su obligación, se estará a la que sea menos gravosa.

En caso en que el oferente viole el deber de buena fe en la etapa previa a la conclusión del contrato o en su celebración o transgreda el deber de información o la legislación de defensa de la competencia o de lealtad comercial, el consumidor tendrá derecho a demandar la nulidad del contrato o la de una o más cláusulas. Cuando el juez declare la nulidad parcial, simultáneamente integrará el contrato, si ello fuera necesario.” El resaltado es mío.

[1289]

Confr. Art. 1105, CCCN.- “Contratos celebrados a distancia. Contratos celebrados a distancia son aquellos concluidos entre un proveedor y un consumidor con el uso exclusivo de medios de comunicación a distancia, entendiéndose por tales los que pueden ser utilizados sin la presencia física simultánea de las partes contratantes. En especial, se consideran los medios postales, electrónicos, telecomunicaciones, así como servicios de radio, televisión o prensa.”

Art. 1106, CCCN.- “Utilización de medios electrónicos. Siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un **soporte electrónico u otra tecnología similar.**”

[1290]

Confr. Carlos Eduardo Tambussi y María Fernanda Yapur, *Régimen de Defensa del Consumidor (I) Introducción...o.c.*, p. 1022.

[1291]

Art. 1107, CCCN.- “Información sobre los medios electrónicos. Si las partes se valen de técnicas de comunicación electrónica o similares para la celebración de un contrato de consumo a distancia, el proveedor debe informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios

para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos.”

[1292]

Art. 1110, CCCN.- “Revocación. En los contratos celebrados fuera de los establecimientos comerciales y a distancia, el consumidor tiene el derecho irrenunciable de revocar la aceptación dentro de los diez días computados a partir de la celebración del contrato.

Si la aceptación es posterior a la entrega del bien, el plazo debe comenzar a correr desde que esta última se produce.

Si el plazo vence en día inhábil, se prorroga hasta el primer día hábil siguiente.

Las cláusulas, pactos o cualquier modalidad aceptada por el consumidor durante este período que tengan por resultado la imposibilidad de ejercer el derecho de revocación se tienen por no escritos.” El resaltado es mío.

[1293]

Art. 1111, CCCN.- “Deber de informar el derecho a la revocación. El proveedor debe informar al consumidor sobre la facultad de revocación mediante su inclusión en caracteres destacados en todo documento que presenta al consumidor en la etapa de negociaciones o en el documento que instrumenta el contrato concluido, ubicada como disposición inmediatamente anterior a la firma del consumidor o usuario. **El derecho de revocación no se extingue si el consumidor no ha sido informado debidamente sobre su derecho.”** El resaltado es mío.

[1294]

Ampliar sobre el cartel de los pañales en el artículo del autor, *Apuntes sobre la nueva regulación de la delación anti-cartel en Colombia y algunas ideas para apuntalar la defensa de la competencia en la República Argentina*, publicado en Diciembre de 2015, Errenews Comercial, N° 38.

[1295]

Los casos de la Comisión Europea contra Microsoft, de 2004 y 2012, son un buen ejemplo. Confr. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_500 disponible al 15/05/2020.

[1296]

Más recientemente, la Comisión Europea multó a Google en casi 1.500 millones de Euros, por abuso de posición dominante en varios mercados. Ampliar en https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770, recuperado el 16/05/2020.

[1297]

Ampliar en [https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA\(2016\)0010_en.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)0010_en.pdf) y <https://hackernoon.com/why-do-voting-systems-need-blockchain-e85e747e906d>, disponible al 02/05/2020.

[1298]

Confr. Thibault Schrepel, *Is blockchain the death of antitrust law? The*

blockchain antitrust paradox, publicado en Georgetown Law Technology Review, N° 281 (2019), Vol. 3.2, disponible en <https://georgetownlawtechreview.org/wp-content/uploads/2019/05/3.1-Schrepel-pp-281-338.pdf>, al 01/05/2020, p. 297.

[1299]

El caso de Microsoft es icónico y una muy buena prueba del argumento presentado. Cuando el Gobierno Federal de EE.UU decidió demandar por monopolización a la empresa de tecnología más valiosa del mundo por aquel momento, se produjo un terremoto. *“Challenging Microsoft was not a popular decision. Microsoft was a well-liked company and Mr. Gates was widely heralded as a visionary genius. Many, Microsoft most of all, argued that **enforcing the antitrust laws against Microsoft would damage innovation and impede the economic growth fueled by the technology sector.** It took the power of law enforcement to rebut Microsoft’s claims that everything it was doing was pro-competitive, innovative and innocent. The discovery of candid internal company memos, a famously revealing deposition of Bill Gates and a full trial made it clear that Microsoft saw the internet as a major threat to its monopoly rule and was seeking to tame it. The presiding judge, Thomas Penfield Jackson of the United States District Court for the District of Columbia, was right to propose that Microsoft be broken into two companies — one for the Windows operating system, one for other products. In the end, unfortunately, Microsoft was kept whole. Some limitations were placed on Microsoft’s behavior, such as a requirement that it share certain programming information with third-party companies. The appropriateness of that remedy is still debated. But what we do know is that the remedy pushed Microsoft to act with more caution, creating an essential opening for a new generation of firms. It might seem like a cruel irony that the immediate beneficiaries of the Microsoft antitrust case — namely, Google, Facebook and Amazon — have now become behemoths themselves. But **this is how the innovation cycle works: It creates room for saplings to grow into giants, but then prevents the new giants from squashing the next generation of saplings.** (Microsoft was itself, in the early 1980s, the beneficiary of another antitrust case, against IBM, the computing colossus of its time.) At a hearing before the Senate, Mark Zuckerberg, the chief executive of Facebook, was asked to name Facebook’s biggest competitor — a company providing a similar service that consumers can go to if they are unhappy with Facebook. Mr. Zuckerberg could not name one. Part of the reason for this is that Facebook bought its most obvious competitors, Instagram and WhatsApp, and continues to acquire upstart companies before they can reach that point.*

The pattern is familiar. And if the Microsoft case showed us anything, it is that we should not trust any one company to decide our future.” Confr. <https://www.nytimes.com/2018/05/18/opinion/microsoft-antitrust-case.html> recuperado el 15/05/2020. Los resaltados son míos.

[1300]

Confr. Thibault Schrepel, *Is blockchain the death of antitrust law? The*

blockchain antitrust paradox, publicado en Georgetown Law Technology Review, N° 281 (2019), Vol. 3.2, disponible en <https://georgetownlawtechreview.org/wp-content/uploads/2019/05/3.1-Schrepel-pp-281-338.pdf>, al 01/05/2020.

[1301] Confr. Thibault Schrepel, *Is blockchain...* o.c. p. 298.

[1302] Idem, p. 300.

[1303] Ampliar en <https://sovrin.org/faq/what-is-self-sovereign-identity/>.

[1304] Idem, 301.

[1305] Ibid.

[1306] Idem, p. 300, nota 96.

[1307] Idem, p. 306.

[1308] Idem, p. 309, nota 130. Afirma Schrepel que “*refusing to provide access to a facility is abusive if it is likely to eliminate all competition on the secondary market, if access is indispensable for entering the market in question, and if access is denied without any objective justification.*” Y agrega: “*Such a refusal to grant access bears similarity to the issue of standard essential patents. Obtaining a license to such patents is deemed essential in order to compete on the market, and for that reason, holders of such patents are strongly encouraged to license them on fair, reasonable, and non-discriminatory (FRAND) terms so as to avoid any breach of antitrust law. One can therefore imagine the development of similar case law in which private blockchain holders will have no choice but to grant access to their blockchains on reasonable and non-discriminatory terms if access to the blockchain is deemed essential to compete. For that reason, a firm that runs an essential private blockchain might soon be prohibited from setting certain access terms which create a strong exclusionary effect. In fact, blockchain gatekeepers (the ones in control of private blockchains) should already consider whether refusing access to third parties is compliant with antitrust law.*” El resultado es mío.

[1309] Idem, p. 312. Afirma Schrepel que “*Tying is the practice of subjecting the sale of one product (or service) to additional sales or obligations. Tying may also entail subjecting a contract to the acceptance of supplementary obligations that have no connection with the original subject of the contract. Blockchain may be used to implement such strategies by subjecting its use to the creation of an account on another platform or to the showing of tokens. This could be seen as anti-competitive.*”

[1310] Idem, p. 313. Schrepel acuñó el término, y lo precisa como: “*Innovation is “the implementation of a new or significantly improved product (good or service).”*”

Accordingly, when the blockchain governance is modified, it could be seen as an innovative practice. In fact, where there is innovation, there is a risk of predatory innovation: “the alteration of one or more technical elements of a product to limit or eliminate competition.” **Predatory innovation appears at first to mirror authentic innovation—it is, after all, a new version of a product or technology—but it is not innovative because it does not bring any real improvements to consumers.** In short, predatory innovation encompasses all anticompetitive strategies that, under the guise of being real innovations, aim at eliminating competition without benefiting consumers or users. While the initial choice of the public or private nature of a blockchain should be exempt from antitrust scrutiny, the type of governance that is chosen implicates the likelihood of anticompetitive practices.” Los resaltados son míos.

[1311]

Idem, p. 316. Sostiene Schrepel que en blockchain “pricing occurs mainly in the form of costly transaction fees when a user is submitting a transaction to be registered into the chain. Predatory pricing is very unlikely on public blockchains because it would only be possible if enough users could be convinced to change the governance structure to facilitate such a change. The situation is quite different for private blockchains. Private blockchains can change the protocol anytime without having to convince anyone to adopt the change. Accordingly, since the protocol can be changed easily, the pricing can also be changed easily in response to competitor pricing. One could imagine, accordingly, that one private blockchain may offer its users very low transaction fees in an attempt to eliminate competing blockchains from the market. The test related to the analysis of predatory pricing, taking into account average variable costs, would then apply”

[1312]

Ibid. Conceptualiza la conducta así: “when a vertically integrated dominant company operates on upstream and downstream markets and sets the upstream price high enough so that companies are unable to sustainably compete in the downstream market”. En blockchains privadas, afirma que “Because they allow income-generating applications while maintaining a financial interest on the platform layer, one can imagine that a strategy of margin squeezing could be implemented. Doing so would require that the dominant company—here the blockchain gatekeeper—changes the price it charges in the upstream market (i.e. the blockchain platform). In the development phase of blockchain, such a strategy seems unlikely, but it will have to be closely monitored in the years to come”.

[1313]

Idem, p. 317. El autor citado define esta práctica anticompetitiva como “the formation of agreements under which customers are contractually required to purchase particular goods or services exclusively from a dominant company. Such terms could be included in the user agreement which is signed before using the blockchain.” En blockchains privadas, “Foreclosing competitors is an efficient way to increase the overall blockchain price for users and developers. Moreover, private blockchains have an interest in increasing their level of attractiveness by obtaining data that they alone can

provide.”

[1314]

Idem, p. 317. Se precisa la conducta como: “grant retroactive rebates or rebates that are conditional on a customer obtaining all or most of its goods or services from the dominant actor. Because all practices are recorded and visible on public blockchains, one user’s discount will be visible to all and granting loyalty rebates or discounts could lead to push-back from users who do not benefit from such a discount. This is more likely to occur if such benefits are perceived as unjustified by other users. Public blockchains therefore push for equal treatment of all users when there is no reason to differentiate among them. Private blockchains do not necessarily benefit from this “visibility effect” because they can determine what information is visible to each user. They may also have a greater commercial incentive to attract reputable users by offering discounts.”

[1315]

Idem, p. 319. En cuanto a los abusos explotativos: “entails directly or indirectly imposing unfair conditions on existing customers or suppliers. Such abuses could be created by the creation of a dual blockchain environment, one for those who pay the most and one for those who pay less and whose transactions may lag behind as a result. An exploitative abuse could occur (...) when blockchain creators provide services in exchange for preferential treatment or when one blockchain imposes unfavorable measures on another blockchain.” Mientras que la discriminación de precios: “Discriminatory abuses occur when parties apply “dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage.” Several kinds of such abuse exist, although price discrimination is the most common (...) it generally occurs in two ways: (i) charging different customers different prices for the same product, or (ii) charging only some customers the same price for different products.”

[1316]

Confr. Thibault Schrepel, *Collusion by blockchain and smart contracts*, publicado en Harvard Journal of Law and Technology, N° 33, vol. 117, 2019, disponible al 02/05/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315182.

[1317]

Ampliar en Michael E. Porter, *How Competitive Forces-Shape Strategy*, 7 HARV. BUS. REV., No. 2 (Mar.-Apr. 1979).

[1318]

Idem, p. 27.

[1319]

Idem, p. 28. Afirma Schrepel que: “**Empirical studies are irrefutable: the more sophisticated the governance, the longer the collusion is lasting. Indeed, about half of collusive agreements die because of internal conflicts between their members; and these conflicts arise mainly after deviant behaviors. Blockchain will help colluders in this regard.**” El resaltado es mío.

[1320] Idem, p. 28. Se sostiene que “*Blockchain makes it possible, via smart contracts, to regulate the price operated by the colluders in order to find a balance point. It can also allow an automatic division of earnings according to predefined criteria, and, of course, it makes it possible to monitor deviant behaviors as well as to punish them, once again by means of smart contracts.*”

[1321] Ibid. Se afirma que “*when firms may observe each other’s actions and interact with one another frequently, tacit collusion may occur and be stable. Public blockchains grant firms access to a large amount, and as such, to observe other colluders’ practices. This will prevent deviant behaviors because the detection risk by other colluders is high. In fact, it is shown that collusion is stable when members have similar interests and can control other colluders’ behavior with mechanisms going beyond mere cheap talks. Of course, the ability to detect cheating is not the only determinant of the cartel duration, and accordingly, blockchain will not make them indefinite. Still, by easing the identification of deviant behaviors, collusive agreements become more stable.*”

[1322] Idem, p. 8.

[1323] Idem, p. 24. Un acuerdo colusivo implementado en blockchain asegura la visibilidad y la trazabilidad del cumplimiento del pacto colusivo. Afirma Schrepel que “*When the blockchain is public, companies can ensure that they have access to all information that is listed in the same place, without any of the users being able to hide this information from others. The blockchain also ensures that the information is certified. This reinforces the trust that users have in each other, hence, the **interest they may find in setting up such an agreement on a blockchain rather than outside it.** In addition, the public nature of the information can greatly complicate the task of antitrust and competition agencies wishing to qualify the agreement. When the blockchain is private, all companies involved in a collusive agreement are getting exclusive and secure access to the information. This can help to strengthen cohesion between them. Private blockchain also allows the information to be certified before being integrated into its network, which, once again, creates a considerable advantage over physical or digital mediums other than blockchain.*” El resaltado es mío.

[1324] Idem, p. 24.

[1325] Idem, p. 12.

[1326] Idem, p. 17. Señala Schrepel que “*The jurisprudence holds that public information sharing only constitutes a cartel when the **information concerns future prices or strategies.** The sharing of actual prices constitutes in itself a “market behavior which does not lessen each undertaking’s uncertainty as to the future attitude of its competitors. At the time when each undertaking engages in such behavior, it cannot be*

sure of the future conduct of the others (...) jurisprudence holds that the **shared data must be capable of reducing “uncertainty related to business behaviour.”** El resaltado es mío.

[1327]

Idem, p. 15. En el Derecho de Defensa de la Competencia, un *acuerdo anticompetitivo ilegal* puede inferirse de “*the existence of the subjective element that characterizes the very concept of an agreement, that is to say a **concurrence of wills between economic operators on the implementation of a policy, the pursuit of an objective, or the adoption of a given line of conduct on the market.***” El resaltado es mío.

[1328]

Idem, p. 20. Grafica Schrepel: “*fewer than 10 mining pools dominated Bitcoin in 2017. In fact, the 7 most powerful ones accounted for more than 85% of all transactions validated on the Bitcoin blockchain. This calls into question the proclaimed decentralized nature of Bitcoin because the owning of more than 51% of mining power is equivalent to a control of the blockchain.*”

[1329]

Idem, p. 21. Schrepel puntualiza las particularidades del Proof Or Work, Proof of Stake, Proof of Activity, Proof of Burn, Proof of Capacity, Proof of Elapsed Time. Agrega: “*To date, Bitcoin and Ethereum, the world’s two leading blockchains, use Proof of Work. The risk of collusive agreements to be created under this consensus is low, although it cannot be eliminated. But things are moving fast in the blockchain “world.” For instance, Ethereum intends to migrate to Proof of Stake where the antitrust risk is more important.*”

[1330]

Idem, p. 23. Precisa Schrepel: “*The developers working on the blockchain’s core software are made up of small groups with a great deal of power over the network, notably that of providing the official software to the verification nodes. This is true, for example, of the Ethereum Foundation and the Bitcoin Foundation whose missions are to promote the protocol of their blockchain. The Bitcoin Foundation also operates by paying certain third parties such as the MIT Digital Currency Initiative, Blockstream, and ChainCode Labs for developing the blockchain. The same goes for private blockchains such as Hyperledger and R3, as they are not open source and have corporate members funding them and contributing to the code according to well-established governance structures. Developers may initiate a hard fork and communicate with miners. Bitcoin uses a mechanism called BIP 9 that allows developers to probe miners about technical changes. Segwit uses another mechanism called BIP 91. And in private blockchains, owners or designated blockchain participants have the authority to resolve discrepancies in the chain which may not be resolved under an objective consensus mechanism, but ask for unilateral intervention by the owners and/or designated participants. It creates control over the blockchain which will foster collusive agreements.*”

[1331] Idem, p. 24. Señala Schrepel: “*depending on the consensus mechanism chosen by the blockchain, the holding of a large part of the tokens may give power to impose decisions and/or coordination with other significant users. **It should be remembered that 1000 people own 40% of the Bitcoin market.** This is often referred to as the Whale Problem. This problem also occurs on the Ethereum blockchain.*”

[1332] Idem, p. 25. Ejemplifica Schrepel: “*companies use blockchain combined with smart contracts to automate the agreement and, in addition, to make it more predictable and transparent. In the case of a public blockchain, smart contracts can be implemented so that the information published on the blockchain serves as parameters for the agreement, which will automatically adjust itself using different types of algorithms. For instance, a smart contract could automate transfers between the colluders and make side payments (...). Moreover, because these smart contracts are coded directly into the blockchain, it will not be possible to modify them without the agreement of the other users. This may only strengthen the stability of the agreement. In the case of a private blockchain, smart contracts may serve the same purpose as described for public blockchains – i.e. governing the relationship between users – and they may also be used to govern the framework of the agreement itself by deciding on the type of information published, its access (that can be modulated upon request) and even its exit conditions. In other words, it is the most sophisticated type of agreement using blockchain.*”

[1333] Idem, p. 26. Afirma Schrepel “*The technology thus makes it possible, particularly through the use of smart contracts, to prevent deviant behaviors. In doing so, it ensures good cohesion to the agreement by **strengthening the trust that colluders have in each other – or, at least, the trust they have in the information on which the collusion is based.** The technology may also be used to correct deviant behaviors by imposing targeted sanctions.*” El resaltado es mío.

[1334] Confr. Thibault Schrepel, *Is blockchain the death of antitrust law?* ...o.c. p. 330.

[1335] Ibid.

[1336] Ibid.

[1337] Idem, p. 331.

[1338] Ibid.

[1339] Idem, p. 333.

[1340] Ibid.

[1341] Idem, p. 333.

[1342] Confr. Patricio Prono y Manuel Usasndizaga, *Derecho Concursal. Noción. Evolución Legislativa Nacional. Principios del Derecho Concursal*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo X, Buenos Aires, 2016, p. 1.

[1343] La Ley de Concursos y Quiebras fue publicada en el Boletín Oficial el 09/08/1995, modificada directamente en ocho oportunidades por las Leyes N° 25.347, 25.563, 25.589, 25.750, 26.086, 26.422, 26.684, 27.170 y finalmente por la Ley N° 26.994, que aprobó el CCCN, que al modificar el régimen general de las obligaciones y tipificar algunos contratos, también impactó indirectamente en la LCQ.

[1344] Confr. Patricio Prono y Manuel Usasndizaga, *Derecho Concursal. Noción. Evolución Legislativa Nacional. Principios del Derecho...o.c.*, p. 13, precisan que los procesos concursales se caracterizan por afectar la totalidad del patrimonio del deudor al momento de la apertura, todos bienes y todas las deudas a tal momento. En caso de quiebra, el deudor queda desapoderado de todos los bienes existentes a la fecha de la declaración de quiebra y de los que adquiera hasta la rehabilitación, salvo bienes exceptuados. Respecto a sus deudas, todas las que tengan causa anterior a la presentación en concurso o a la declaración de quiebra quedan comprendidas, incluso si son ilícitas, condicionales, litigiosas, no vencidas o ignoradas.

[1345] Idem, p. 15. Los acreedores pasan a formar una masa, la masa de acreedores, y salvo las ejecuciones reales, a todos ellos se le suspenden los juicios iniciados y se les prohíbe iniciar nuevos a partir de la presentación en concurso de su deudor, o de su quiebra.

[1346] Idem, p. 17. Todo acreedor de causa o título anterior al concurso o la quiebra que pretenda cobrar su crédito, tiene la carga procesal de concurrir al proceso concursal y verificar su crédito. Si ningún acreedor concurre a verificar su crédito, finaliza el proceso. La igualdad de los acreedores es quizás el principio más emblemático: *par conditio creditorum*. Al proceso concursal le corresponde asegurar que la desgracia del deudor sea distribuida equitativamente entre todos los acreedores. Se trata de un principio no absoluto, ya que la ley puede otorgar soluciones diferentes a quienes se encuentren en distintas situaciones, e.g. empleados en relación de dependencia, y además existe el régimen de privilegios de los Arts. 241 y 246, LCQ, régimen que permite que algunos acreedores sufran menos ante la desgracia de la cesión de pagos de su deudor.

[1347] Idem, p. 21. El juez concursal impulsa de oficio el proceso una vez peticionada

la apertura del concurso o el pedido de quiebra, no depende del síndico, ni del propio deudor, para avanzar. Resáltese la facultad del juez de declarar inoponibles los actos enumerados en el Art. 118 LCQ celebrados durante el período de sospecha del Art. 116 LCQ, o la facultad de continuar un contrato con prestaciones recíprocas pendientes con prescindencia de la voluntad del fallido, del tercero contratante, ni del síndico, confr. Art. 144, LCQ.

[1348]

Idem, p. 23. El juez puede ordenar las medidas de investigación que considere necesarias para esclarecer la situación patrimonial del deudor. Este principio permite que un juez rechace el pedido de concurso al propio deudor si, en opinión del juez, no se cumple la cesación de pagos que la ley exige.

[1349]

Idem, p. 24. Si un deudor atraviesa el concurso y la quiebra de manera sucesiva, tal sucesión de procedimientos se rige por el principio de unidad, como si fueran un único proceso.

[1350]

Idem, p. 25. *Principio u objetivo* del régimen falencial, es una cuestión discutible. Este principio puede permitir que se posterguen intereses individuales –del mismo deudor, de sus acreedores– en aras de conservar la empresa, dada su función social. Se lo aprecia operar en los arts. 24, 126, 193, 195, 204 LCQ.

[1351]

Idem, p. 622. La LCQ regula también el acuerdo preventivo extrajudicial, un acuerdo privado entre el deudor y sus acreedores que, de ser homologado, se torna oponible a todos los acreedores. Son procesos de reestructuración con intervención judicial limitada, dando lugar a negociaciones rápidas y directas, con menores costos. Puede ser considerado un concurso preventivo flexibilizado, o un contrato sui generis, ya que finaliza en sede concursal. Ampliar, en general, en o.c., p. 628.

[1352]

Idem, p. 550. Se trata de una propuesta por terceros, y es la posibilidad que reconoce la LCQ de que, ante la no obtención de las mayorías necesarias para homologar una propuesta de acuerdo preventivo dentro del período de exclusividad, terceros puedan formular ofertas a los acreedores. El instituto está reglado en el Art. 48 LCQ. Al permitir que cualquier tercero pueda ofertar a los acreedores del deudor un plan de pagos, si éstos aceptaran, entonces los socios de la sociedad concursada deberán *forzosamente* vender las participaciones sociales al tercero ofertante que consiguió las mayorías legales. Es una transferencia ex lege del capital social: la sociedad es la misma, cambian sus dueños. Evidentemente, es un instituto que encarna el principio de conservación de la empresa, ya que procura evitar la quiebra. Los terceros que participan pueden o no ser acreedores de la concursada, y busca evitar la liquidación de la empresa para pagar sus pasivos. El cambio de dueños de la concursada se produce por una sentencia judicial, y es algo distinto a una venta forzada o una expropiación. Es un instituto propiamente concursal. Se trata de un

procedimiento cuya apertura no depende del deudor, por tanto es imperativo.

[1353]

Idem, p. 30.

[1354]

Ibid. El derecho concursal está mutando hacia un derecho de prevención de las crisis empresarias, que opera mucho antes de que la cesación de pagos se manifieste, y en esa dirección se inscriben los acuerdos preventivos extrajudiciales y su reconocimiento legal. Sin embargo, hoy por hoy, la cesación de pagos sigue definiendo el acceso o no a los procesos concursales, y es entendida como un estado patrimonial generalizado y permanente que refleja la imposibilidad de un sujeto de pagar de manera regular obligaciones exigibles, cualquiera sea su naturaleza y las causas que lo generen.

[1355]

Idem, p. 151. Su actividad es típica y necesaria, es un *órgano* profesional, experto e idóneo en la materia concursal, que actúa cumpliendo deberes y con facultades que son definidas por la ley. Es un órgano del concurso, pero no es un funcionario público: es un auxiliar de la justicia. Existen sindicaturas individuales (categorías A) y por estudio de síndicos (categoría B), y se asignan según la complejidad de cada concurso/quiebra. Sólo los contadores públicos pueden ser síndicos.

[1356]

Idem, p. 248. Las normas que regulan los efectos del concurso son de orden público. A su vez, existen efectos que se producen desde la presentación del concurso, efectos que se producen desde la apertura del concurso, y efectos que se producen desde la publicación de edictos. Muchos efectos, a su vez, concluyen con la homologación del acuerdo, mientras que otros subsistirán junto con los efectos del acuerdo homologado.

[1357]

Idem, p. 250. El deudor sigue administrado su patrimonio, pero con ciertas restricciones. En la quiebra, en cambio, el deudor pierde la administración de su patrimonio, por efecto del desapoderamiento. El concursado puede realizar operaciones normales de su giro empresarial, i.e. actos de administración, sin necesidad de previa autorización judicial, pero, los actos de disposición o que exceden la administración ordinaria requieren previa autorización –e.g., excede la administración ordinaria decidir no ejercer el derecho de suscripción preferente que le asiste a la concursada–, y están prohibidos los actos a título gratuito y de disposición que impliquen alterar la situación de los acreedores por causa o título anterior a la presentación del concurso. Los acreedores con privilegio especial de causa anterior al concurso pueden ejecutar sus garantías.

[1358]

Idem, p. 262. La presentación del concurso congela el pasivo a la fecha de la presentación, para dar certeza acerca de la participación que tendrán los acreedores en la decisión de aprobar o no la propuesta del deudor. Se frenan todos los intereses, de

cualquier naturaleza, incluidos los de una cláusula penal, pero la medida no beneficia a los fiadores del concursado. No se frenan los mecanismos de actualización del capital. Los créditos con garantía prendaria o hipotecaria siguen devengando intereses; en la quiebra la situación es distinta, confr. Art. 129 LCQ, al igual que los créditos laborales que siguen generando intereses moratorios, que gozan de privilegio general.

[1359]

Idem, p. 268. Las obligaciones de hacer y no hacer, y las de dar moneda extranjera, deben convertirse a moneda de curso legal. En el caso de moneda extranjera, la conversión es sólo al efecto de calcular el pasivo para calcular las mayorías, es por tanto provisoria, a los fines del voto, y no del pago. Distinto es el caso en la quiebra, confr. Art. 127 LCQ.

[1360]

Idem, p. 270. La compensación está prevista para la quiebra, confr. Art. 130 LCQ, y la doctrina entiende que se aplica al concurso, si se produjo *antes* de la apertura del concurso.

[1361]

Idem, p. 271. El concurso preventivo no produce el vencimiento anticipado de todos los plazos pero habilita al acreedor a verificar su crédito –como crédito condicional–, confr. Art. 353 CCCN; lo contrario ocurre en la quiebra, confr. Art. 128, LCQ, ya que la imposibilidad de pagar es total y definitiva, no tiene sentido aguardar al vencimiento del plazo. La regla de la no caducidad de plazos en el concurso preventivo se aplica a todo acreedor por título o causa anterior a la presentación, sin importar si es acreedor privilegiado. Si el acreedor no verifica su crédito, el concursado no podrá pagar; aún verificado, el pago debiera ser autorizado.

[1362]

Idem, p. 273. El instituto está reglado en la quiebra, confr. Art. 131 LCQ. En el concurso, en cambio, no está expresamente regulado, pero se considera que es aplicable analógicamente, con lo cual la presentación del concurso suspende el derecho de retención del acreedor del concursado.

[1363]

Idem, p. 290. Este instituto procura la rápida cancelación de los créditos laborales con privilegio especial y general, dada su naturaleza alimentaria, permitiendo su pago anticipado sin necesidad de verificar la acreencia, suplantando la típica vía de ingreso al pasivo del deudor.

[1364]

Idem, p. 305. Estos efectos procesales afectan a los procesos judiciales donde se reclaman deudas al concursado con causa anterior a la presentación concursal, atrayéndolos al juez concursal en función de la superioridad de intereses tutelados por el proceso falencial y la igualdad de trato a los acreedores, en tanto y en cuanto el juicio en cuestión tenga contenido patrimonial, y sujeto a ciertas excepciones legales. En los procesos que no se atraen al concurso, i.e. los de conocimiento en trámite, en los juicios laborales y en procesos en los que el concursado integra un litis consorcio pasivo necesario, no pueden dictarse medidas cautelares y deben levantarse las

dictadas, sin importar si el embargante es un acreedor privilegiado o quirografario. Los acreedores con garantía real ejecutable extrajudicialmente pueden continuar con el trámite de liquidación, confr. Art. 23 LCQ, sus procesos no se suspenden, no deben verificar su crédito, pero deben rendir cuentas sobre el resultado de la realización del bien por vía incidental. Todo remanente debe depositarse a la orden del concurso. Son los acreedores que tienen una prenda común, o que son bancos o acreedores con prenda con registro, o el acreedor hipotecario cuando ejecuta letras hipotecarias, y el titular de un warrant. Si el remate ocurrirá luego de publicados los edictos de apertura de concurso, el acreedor deberá presentarse al juez y comunicar la fecha de la subasta, además de acompañar el título de su crédito. Este aviso no se sustancia, y su omisión implica la nulidad del remate.

Ahora bien, el mismo Art. 23 LCQ permite al juez del concurso, a pedido del concursado, suspender por hasta 90 días hábiles judiciales estos remates judiciales y extrajudiciales instados por acreedores privilegiados, incluyendo el secuestro. La conservación del bien debe ser imprescindible para las actividades de la concursada. Mientras dura la suspensión, el crédito genera intereses, que tienen rango de gastos de conservación y justicia, confr. Art. 240 LCQ. Esta decisión es apelable con efecto devolutivo.

[\[1365\]](#)

El Art. 20 LCQ reza: “Contratos con prestación recíproca pendiente. El deudor puede continuar con el cumplimiento de los contratos en curso de ejecución, cuando hubiere prestaciones recíprocas pendientes. Para ello debe requerir autorización del juez, quien resuelve previa vista al síndico. La continuación del contrato autoriza al cocontratante a exigir el cumplimiento de las prestaciones adeudadas a la fecha de presentación en concurso bajo apercibimiento de resolución.

Las prestaciones que el tercero cumpla después de la presentación en concurso preventivo, y previo cumplimiento de lo dispuesto en este precepto, gozan del privilegio previsto por el artículo 240. La tradición simbólica anterior a la presentación, no importa cumplimiento de la prestación a los fines de este artículo.

Sin perjuicio de la aplicación del *artículo 753 del Código Civil*, el tercero puede resolver el contrato cuando no se le hubiere comunicado la decisión de continuarlo, luego de los treinta (30) días de abierto el concurso. Debe notificar al deudor y al síndico.

Servicios públicos. No pueden suspenderse los servicios públicos que se presten al deudor por deudas con origen en fecha anterior a la de la apertura del concurso. Los servicios prestados con posterioridad a la apertura del concurso deben abonarse a sus respectivos vencimientos y pueden suspenderse en caso de incumplimiento mediante el procedimiento previsto en las normas que rigen sus respectivas prestaciones.

En caso de liquidación en la quiebra, los créditos que se generen por las prestaciones mencionadas en el párrafo anterior gozan de la preferencia establecida por el artículo 240.” El resaltado, en tanto reenvía a un artículo derogado, no tiene efecto legal alguno.

[1366] Idem, p. 276. Al ser una regla de orden público, las estipulaciones contractuales que la contradigan son nulas, sin perjuicio de la validez del contrato que las contenga.

[1367] Idem, p. 277. Éstos contratos son de ejecución diferida –por existencia de un plazo–, o bien de tracto sucesivo o ejecución continuada, aquellos en los que las obligaciones de las partes son exigibles durante toda su duración, encontrándose las partes obligadas recíprocamente. Ambos quedan incluidos dentro del Art. 20 LCQ. Quedan también comprendidos los contratos de larga duración, confr. Art. 1011, CCCN.

[1368] Idem, p. 279. La norma no permitiría al concursado solicitar al juez la resolución del contrato, pero la doctrina entiende que tal facultad también fluye de la exégesis del artículo 20. Resolver un contrato puede ser tan importante como continuarlo.

[1369] Ibid.

[1370] Idem, p. 281. El principal beneficio es poder exigir el cumplimiento de las prestaciones adeudadas a la fecha del concurso, sin tener que verificarlas. A su vez, las prestaciones cumplidas en el marco de la continuación forzada del contrato tienen el carácter de gastos de conservación y justicia, confr. Art. 240 LCQ, por lo cual no se suspenden a su respecto los intereses, ni se convierten a moneda nacional.

[1371] Idem, p. 283.

[1372] Ibid.

[1373] Idem, p. 284.

[1374] Ibid. Por aplicación del Art. 1171, CCCN. El acreedor de la obligación de escriturar deberá verificar su crédito, y es un caso en que no aplica la conversión de obligaciones no dinerarias.

[1375] Idem, p. 286. Es un contrato fluyente, sea que el concursado sea locador o locatario.

[1376] Ibid. El leasing tiene una regulación especial contenida en la Ley N° 25.248.

[1377] Idem, p. 287. Son todos ejemplos de contratos con prestaciones recíprocas y de tracto sucesivo.

[1378] Ibid. El Art. 1623 CCCN regula el caso. La cesión de derechos es eficaz frente a los acreedores del concursado si es notificada al deudor cedido antes de la fecha de la presentación en concurso.

[1379]

Idem, p. 288. Si bien son contratos de ejecución continuada, no son contratos con prestaciones recíprocas pendientes, sino contratos plurilaterales de organización. Aplican los Arts. 1461, 1464 y 1469, y 1478, CCCN, a la agrupación de colaboración, a la unión transitoria y al consorcio de cooperación, respectivamente.

[1380]

Ibid. La presentación en concurso del cuentacorrentista no es causal de extinción del contrato; sí lo es su quiebra, confr. Art. 1404 CCCN y Art. 147, LCQ. Lo normal, sin embargo, es que los bancos cierren las cuentas, lo que obliga al concursado a adentarse y ejercer la opción del Art. 20 LCQ, solicitando medidas cautelares que impidan el cierre de las cuentas por el solo hecho del concurso.

[1381]

Confr. Art. 88, LCQ.

[1382]

Idem, p. 721. La sentencia de quiebra produce la inhibición general del fallido, para evitar que disponga de los bienes de su propiedad. Es una consecuencia del desapoderamiento.

[1383]

Idem, p. 723. Los pagos por terceros al fallido son ineficaces por consecuencia del desapoderamiento, salvo que hayan ingresado al activo liquidable.

[1384]

Ibid. Las comunicaciones dirigidas al fallido deben ser entregadas al síndico, pero ello no implica interceptar las comunicaciones enviadas por el fallido a terceras personas. La doctrina afirma que la interceptación debiera incluir los correos electrónicos.

[1385]

Idem, p. 724. Suele ser la misma sindicatura la que realiza el inventario al momento de efectuar la incautación.

[1386]

Idem, p. 744. El desapoderamiento se mantendrá mientras dura la inhabilitación, es decir, durante un año desde dictada la sentencia de quiebra, plazo que puede ser reducido, dejado sin efecto y también prorrogado. A los bienes a desapoderar se agregarán aquellos que hayan salido del patrimonio del fallido dentro del período de sospecha y sean objeto de acciones de ineficacia concursal, o simulación o fraude común. La incautación debe ser inmediata a la sentencia de quiebra.

[1387]

Idem, p. 744.

[1388]

Quedan fuera del desapoderamiento: (i) los derechos no patrimoniales, (ii) los bienes inembargables regulados en el Art. 744, CCCN, (iii) indemnizaciones por daños materiales o morales; y (iv) ciertos bienes excluidos por otras leyes, como la vivienda familiar.

[1389] Idem, p. 763.

[1390] Idem, p. 901.

[1391] Idem, p. 905.

[1392] Idem, 908. El período que inicia con el estado de cesación de pagos y que finaliza con la sentencia que lo declara, o con la presentación en concurso, se llama período de sospecha, y su fecha de inicio es determinada por el juez, confr. Art. 115, 117, LCQ, pudiendo extenderse hasta 2 años antes de la presentación en concurso o de la sentencia de quiebra, según corresponda.

[1393] Idem, p. 907. Usandizaga, o.c., p. 958 precisa que el tercero cocontratante deber restituir lo recibido *in natura*, y si ello no fuera posible, deberá pagar el valor del bien recibido oportunamente.

[1394] Idem, p. 922. Es perjudicial todo acto del fallido que empeore las posibilidades de cobro de los acreedores, generalmente al disminuir la garantía patrimonial del deudor, o por violar la *par conditio creditorum*.

[1395] El Art. 118 LCQ taxativamente regula los casos en que la inoponibilidad procede de pleno derecho: “*Son ineficaces respecto de los acreedores los actos realizados por el deudor en el período de sospecha, que consistan en: 1) Actos a título gratuito; 2) Pago anticipado de deudas cuyo vencimiento según el título debía producirse en el día de la quiebra o con posterioridad; 3) Constitución de hipoteca o prenda o cualquier otra preferencia, respecto de obligación no vencida que originariamente no tenía esa garantía.*

La declaración de ineficacia se pronuncia sin necesidad de acción o petición o expresa y sin tramitación. La resolución es apelable y recurrible por vía incidental.” El resaltado es mío. Se sostiene, en o.c., p. 924, que el tercero *puede demostrar* que el activo del deudor es suficiente para cubrir sus deudas, e impedir así la declaración de inoponibilidad que lo afecta. En punto a los actos a título gratuito, cabría incluir aquí el hecho de entregar a un tercero la llave privada, secreta, de titularidad del fallido.

En relación a la constitución de *preferencias* a favor de un acreedor que antes no tenía ninguna garantía: sostiene Usandizaga que la norma incluye cualquier garantía constituida por el deudor, siendo sólo ejemplos la prenda y la hipoteca, e incluyendo mejoras como reducción de plazos, reconocimiento de intereses no previstos *ab initio* o aumentos en la tasa de interés.

Durante la vigencia de la Ley N° 19.551, el pago por entrega de bienes era también un acto inoponible de pleno derecho. La LCQ cambió el criterio: tal pago puede ser atacado, pero vía Art. 119 LCQ, por lo que deberá probarse el conocimiento del estado de cesación de pagos en quién lo recibió. La situación está vinculada al Art. 122 LCQ:

pago efectuado a favor del acreedor peticionante de la quiebra por un tercero no interesado. En estos casos, se presume *iuris et de iure* que el tercero conocía el estado de cesación de pagos. El acreedor que haya recibido bienes en tal hipótesis debe restituir lo recibido, y el tercero que haya pagado no puede subrogarse en los derechos del acreedor, deberá reclamar al fallido lo abonado, confr. o.c. p. 941.

[1396] El Art. 119 LCQ regula el caso, y requiere que el tercero *conociere* el estado de cesación de pagos del deudor al momento de celebrar el contrato, existiendo la posibilidad de que el tercero demuestre que el acto *no causó perjuicio a la masa acreedora*. Estas acciones no proceden de oficio, sino que requieren un trámite ordinario. El conocimiento –i.e. la *cognoscibilidad*– del tercero debe demostrarse, cuestión nada sencilla, y en la que vale recurrir a presunciones e indicios.

[1397] Confr. Manuel Usandizaga, *Acciones de recomposición patrimonial (I): inoponibilidad concursal*, en en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo X, Buenos Aires, 2016, p. 925.

[1398] Confr. Renato Mangano, *Blockchain securities, insolvency law and the sandbox approach...*o.c. p. 715.

[1399] Idem, p. 717.

[1400] Idem, p. 720.

[1401] Idem, p. 721.

[1402] Idem, p. 722.

[1403] Idem, p. 723.

[1404] Confr. Alan Rosenberg, *Automatic contracts and the Automatic Stay, a primer on “smart contracts” in Bankruptcy*, recuperado el 05/05/2020 en http://www.mrthlaw.com/wp-content/uploads/2019/07/feature1_07-19.pdf.

[1405] Ibid. Afirma el autor citado, con relación a los actos ineficaces en la quiebra por conocimiento de la cesión de pagos, que: “*the automatic stay prevents “any act to obtain possession of property of the estate or of property from the estate or to exercise control over property of the estate,” as well as “any act to collect, assess, or recover a claim against the debtor that arose before the commencement of the case.”* To deter stay violations, the Code imposes harsh penalties. Moreover, “**an individual injured by any willful violation of a stay ... shall recover actual damages, including costs and attorneys’ fees, and, in appropriate circumstances, may recover punitive damages.**” As such, ‘Willfulness,’ for purposes of being subject to damages ... for

violating the automatic stay, does not mean that one intends to violate specific provisions of the Bankruptcy Code, but that there is 'deliberateness of conduct' coupled with knowledge of the bankruptcy filing." El resaltado es mío.

[1406]

Ibid.

[1407]

Confr. <https://media.consensys.net/controlling-autonomy-a-new-tool-to-stop-smart-contracts-once-executed-bc9de699bca0>, recuperado el 05/05/2020.

[1408]

Ibid.

[1409]

Ley de Protección de los Datos Personales N° 25.326, publicada en el Boletín Oficial el 02/11/2000. Con fecha 19/09/2018 se presentó al Congreso un proyecto de nueva ley de protección de datos personales, cuyo texto está disponible, al 03/05/2020, en el siguiente link:

https://www.argentina.gob.ar/sites/default/files/mensaje_nde_g_147-2018_datos_personales.pdf.

[1410]

La Ley N° 27.275, publicada en el Boletín Oficial el 29/09/2016, reglamenta el derecho al acceso a la información pública. En su Art. 19, creó la Agencia de Acceso a la Información Pública como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS. Esta Agencia fue designada Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326.

[1411]

La Ley N° 27.483 fue publicada en el Boletín Oficial el 02/01/2019 y aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscrito en la ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981, que consta de veintisiete (27) artículos y el Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las autoridades de control y a los flujos transfronterizos de datos, suscrito en la ciudad de Estrasburgo, República Francesa, el día 8 de noviembre de 2001, que consta de tres (3) artículos. El texto de dicho Convenio está disponible, al 03/05/2020, en el siguiente link: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318245/ley27483.pdf>.

[1412]

Confr. Carolina Abdelnabe Vila, *Argentina se adapta a la normativa europea...* o.c. destaca las siguientes Resoluciones: Resolución N° 40/2018 referente a la Política Modelo de Protección de Datos Personales para Organismos Públicos y al Delegado de Protección de Datos Personales; Resolución N°47/2018 sobre Medidas de Seguridad; Resolución N° 132/2018 referente a la Inscripción de las Bases de Datos y la Resolución N° 159/2018, mediante la cual se aprobó unos lineamientos y contenidos

básicos que las empresas pueden incorporar a sus normas autorregulatorias y de esa manera, realizar transferencias internacionales hacia empresas que conformen un mismo grupo económico ubicadas en países sin legislación adecuada para la protección de datos personales.

[1413]

La Resol. 9/2019 fue dictada por la Agencia de Acceso a la Información Pública y publicada en el Boletín Oficial el 16/01/2019. Al 03/05/2020 está disponible aquí: <http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=318874>. La Resol. 9/19 contiene los llamados *criterios orientadores e indicadores de mejores prácticas* en la aplicación de la Ley de Protección de Datos Personales N° 25.326.

[1414]

Confr. Carolina Abdelnabe Vila, *Argentina se adapta a la normativa europea, mientras espera la sanción de la nueva Ley de Protección de Datos Personales*, disponible al 03/05/2020 en <https://www.abogados.com.ar/argentina-se-adapta-a-la-normativa-europea-mientras-espera-la-sancion-de-la-nueva-ley-de-proteccion-de-datos-personales/22921>.

[1415]

Véase *supra*, en 1.1.8.2.3.

[1416]

Una forma posible de armonización es la propuesta por la Blockchain Federal Argentina. Véase *supra* en 3.5.1.4.2.

[1417]

Constitución Nacional, Art. 43: “Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o

en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio.” El resaltado es mío.

[1418]

Confr. Mercedes Eugenia López, *El habeas data en el derecho constitucional argentino. Concepto y alcances. Recepción jurisprudencial*, publicado en elDial DC2510, el 05/07/2018.

[1419]

Ibid.

[1420]

Ibid.

[1421]

Ibid. Afirma López, o.c., que en ambos casos mediante una acción de habeas data se pretendía borrar información sobre deudas bancarias con fundamento en el Art. 26 de la Ley N° 25.326 (CSJN, 8/11/2011, C.1380 “Catania v. BCRA s/habeas data” y CSJN, 8/11/2011, N.112, “Napoli, Carlos v. Citibank N.A. s/habeas data”). En Catania, el Alto Tribunal sostuvo, que en materia de derecho al olvido “no resulta del texto de la ley –ni puede inferirse de su génesis– que el plazo de cinco años deba quedar pospuesto mientras la deuda sea exigible por no haberse operado a su respecto la prescripción”.

Destacó también que la Ley N° 25.326 “ha consagrado el derecho del afectado a exigir que –transcurrido cierto tiempo– los datos significativos para evaluar su solvencia económica-financiera no sean mantenidos en las bases ni difundidos, con el objeto de que el individuo no quede sujeto indefinidamente a una indagación sobre su pasado”.

En el caso “Catania” un particular solicitó, mediante un habeas data, la supresión de información crediticia adversa por haber transcurrido el plazo de cinco años que prevé la Ley N° 25.326. Se trató del primer caso en que el Máximo Tribunal se pronuncia sobre este tema. En primera y segunda instancia su planteo fue rechazado. Los magistrados que intervinieron alegaron que la falta de pago de la deuda impedía la supresión de la información hasta que hubiera operado la prescripción.

El Máximo Tribunal sostuvo que la idea del legislador fue fijar un plazo de 5 años y que el plazo del derecho al olvido corre en forma separada de otros plazos como la prescripción, o de otras situaciones como la vigencia de la deuda o su exigibilidad. No hay que esperar que la deuda esté prescrita, de lo contrario se desvirtúa la voluntad del legislador. En este caso la Corte Suprema revoca la sentencia y manda dictar nuevo fallo en atención a que el tribunal había rechazado el habeas data porque había considerado que las deudas estaban vigentes y ello impedía el *olvido* de las mismas.

[1422]

Ibid. Remarca López, o.c. que en Napoli, la Corte vuelve, el mismo día, a tratar el tema del derecho al olvido, en especial respecto a desde cuándo se debe contar el plazo de 5 años. La discusión se centró en *la fecha en que debe comenzar a computarse el plazo de cinco años establecido por la Ley N° 25.326*. En este supuesto, la Cámara

Federal que intervino falló de modo favorable al actor. En ambos casos, el Alto Tribunal nacional realizó un examen general de las normas aplicables, es decir, de la Ley N° 25.326 y su decreto reglamentario. Luego, se abocó a develar la intención del legislador al consagrar el llamado “derecho al olvido”. De modo puntual, el Máximo Tribunal destacó que “más allá de las bondades, o no, del sistema ideado, **el legislador expuso su preocupación acerca de que el mantenimiento de información adversa en las pertinentes bases de datos durante un largo lapso podría dar lugar a una suerte de inhabilitación del deudor y a la consiguiente imposibilidad de reingreso al circuito comercial**”. Por su parte, en el caso “Catania”, la Corte explicó que la Ley N° 25.326 distingue “la situación de aquellos deudores que no han cancelado sus deudas (en cuyo caso el plazo será de 5 años), de los que sí lo han hecho (supuesto en que el plazo se reduce a 2 años), con total independencia de que en relación a los primeros pueda perseguirse el cobro de la acreencia mientras la obligación sea jurídicamente exigible”. Ahora bien, respecto del cómputo del plazo de cinco años, cuestión especialmente debatida en el caso “Napoli”, el Alto Tribunal remarcó que el decreto reglamentario que regulaba la cuestión era “impreciso” y “poco claro” lo que ameritaba que se subsane el problema mediante “una interpretación que, sin excluir su literalidad, se ajuste estrictamente a la voluntad del legislador que dictó la Ley 25.326”. “Ha de evitarse toda inteligencia que en los hechos implique una postergación sine die, o una excesiva tardanza en el inicio del cómputo del plazo que se examina, puesto que ello se opone al declarado propósito de lograr una reinserción del afectado en el circuito comercial o financiero”, puntualizó en “Napoli” el Alto Tribunal. Ahora bien, el derecho al olvido tiene otras aristas relacionadas con la libertad de información y la libertad de prensa. Con las redes globales como Internet el derecho al olvido cobra dimensiones insospechadas frente al poder omnipresente de los buscadores y de las redes sociales que todo lo conectan y revelan. En este sentido, la Máximo Tribunal ha ido diseñando su doctrina a la luz de los derechos a la libertad de expresión y a la privacidad en la Sociedad de la Información en los sucesivos precedentes que ha dictado y cuyo estudio excede este análisis.

[\[1423\]](#)

Confr. Arnaldo Casilino, *Derecho al olvido a la europea*, publicado en el Dial DC1D23, con fecha 07/16/2014, quien afirma: “El “derecho al olvido”, que no está explícitamente legislado de ese modo, proviene de las normas de protección de datos que, palabras más, palabras menos, postulan que sólo se pueden conservar ciertos datos para medir la solvencia económica por un determinado plazo.

En la Ley Española 15/99, art. 29 inc. 4, por ejemplo, ese plazo es de seis años. La Ley nacional 25.326, art. 26, punto 4, lo reduce a cinco (5) años, y dos (2) en caso de cancelación o extinción de la deuda.

Como vemos, se trata de una regulación específica, para una situación puntual, como son los informes crediticios. De hecho, el fallo “Costeja” también deriva de una antigua deuda, aparentemente ya saldada.” El autor citado cita varios precedentes donde se

rechazaron pedidos de “olvido”: *in re* “A, R. H. c/ S.A. La Nación y Google”, se rechazó una medida cautelar innovativa tendiente a eliminar el enlace a una nota de opinión publicada en el año 2001, que hacía referencia al peticionario involucrándolo en un hecho delictivo, priorizándose el derecho a la libertad de expresión. *In re* “C., E. J. c/ Google Inc. s/ habeas data”, se rechazó una demanda que pretendía eliminar del buscador ciertos enlaces que relacionaban a la actora con artículos periodísticos publicados en el diario Página/12, relativos a la quiebra fraudulenta de una conocida entidad financiera, afirmando que “la eliminación de la dirección de URL importaría una censura a la libertad de expresión no solo al proveedor del contenido sino a la publicación originaria, ya que con el fin de desvincular el dato manifiestamente incorrecto, se bloquearía el ingreso a la totalidad de la nota propiedad de Página 12, la cual no aparece palmariamente falsa o incorrecta.” *In re* “D. S., D. A. c/ Grupo Clarín, Google y otros s/ habeas data”, el actor también pretendía el bloqueo de ciertos enlaces a notas que lo involucraban en una investigación judicial por narcotráfico. El actor acreditó que había sido sobreseído en la causa. Pero el Juzgado Civil y Comercial Federal N° 4 rechazó la acción “...teniendo en cuenta que, como se dijo, las notas periodísticas cuestionadas, obrantes en los sitios web indicados, son el reflejo de información exacta al momento de su publicación, no corresponde que aquellas sean suprimidas y/o actualizadas”. *In re* “M., F. c/ Google Argentina SRL s/ Habeas Data”, el actor pretendía el bloqueo de acceso a una nota periodística alojada en el diario Página/12, que informaba sobre su procesamiento en una causa iniciada por el ex Director General de Aduanas. Aquí también el actor acreditó su sobreseimiento definitivo recaído posteriormente en la causa. El Juzgado Civil N° 66 rechazó la demanda, indicando que “...estas ediciones que fueron noticia posteriormente constituyen el **‘Archivo del Diario’, que es inmutable, tanto como lo son todos los periódicos en soporte papel ya publicados por la Editorial;** de procederse a la eliminación de la publicación en la página web se estaría provocando un acto de censura que impide a la ciudadanía el derecho a buscar información en Internet y acceder a ella, lo que importa la violación de la garantía constitucional de la libertad de expresión conforme lo establece el art. 1 de la Ley 26.032.

[\[1424\]](#)

Confr. Eduardo Molina Quiroga, *Derecho al olvido en la interpretación de la Corte*, publicado en elDial DC1782 con fecha 12/06/2011. Afirma Molina Quiroga que: “Como hemos sostenido desde hace tiempo, la autodeterminación informativa excede ampliamente el ámbito de los llamados datos sensibles, y su adecuada tutela impacta fuertemente en la actividad económica. **Los informes crediticios constituyen una especie del género datos personales, que pueden revestir al menos dos modalidades. Una es la que se limita a registrar el cumplimiento o incumplimiento de obligaciones, que hemos asimilado a un dato de balance, en el sentido de su configuración lógica (es verdadero o falso). La otra variedad, que es la más útil para medir el riesgo de crédito, son los informes sobre solvencia, que constituyen una**

operación compleja, que articula diversos datos e incluye un juicio de valor. Aunque la primera esté necesariamente imbricada en la segunda, es inaceptable que se establezca el grado de riesgo de una persona en base, exclusivamente, a su incumplimiento de una obligación, la existencia de una deuda o de una demanda en su contra. Actuar de este modo implica malversar una norma destinada a proteger los datos personales y convertirla en un mecanismo de cobro extrajudicial de deudas cuya persecución judicial resulta poco rentable. **Creemos que la prolongación indebida de archivos sobre datos referidos al incumplimiento de obligaciones –en la mayoría de los casos- tiene por finalidad obtener el cobro de la deuda mediante la información de la misma, desconociendo deliberadamente el llamado “derecho al olvido”.** El resaltado es mío.

[1425]

In re: “Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González”, disponible al 03/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0131>, anotado por Arnaldo Casilino, *Derecho al olvido a la europea*, publicado en elDial DC1D23, con fecha 07/16/2014, quien puntualiza: “El Tribunal de Justicia de Europa estableció que las personas tienen derecho a solicitar a un motor de búsqueda de Internet (Google u otro) la eliminación de ciertas referencias o enlaces que aparecen al ingresar su nombre como objeto de búsqueda, aun cuando: (a) la información correspondiente no haya sido eliminada del sitio web original que la contiene; (b) la información sea verdadera, e inclusive fuera publicada en su momento por mandato legal; (c) el solicitante ni siquiera demuestre que la información le causa un daño cierto. Esta petición únicamente puede ser formulada por una persona física.”

[1426]

In re “DENEGRI, NATALIA RUTH c/ GOOGLE INC. s/ DERECHOS PERSONALÍSIMOS: ACCIONES RELACIONADAS”, disponible al 03/05/2020 en <https://www.diariojudicial.com/public/documentos/000/088/642/000088642.pdf>.

[1427]

Confr. proyecto de nueva ley de protección de datos personales, cuyo texto está disponible, al 03/05/2020, en el siguiente link: https://www.argentina.gob.ar/sites/default/files/mensaje_nde_g_147-2018_datos_personales.pdf.

[1428]

Ibid.

[1429]

La Resol. 9/2019 fue dictada por la Agencia de Acceso a la Información Pública y publicada en el Boletín Oficial el 16/01/2019. Al 03/05/2020 está disponible aquí: <http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=318874>. La Resol. 9/19 contiene los llamados *criterios orientadores e indicadores de mejores prácticas* en la aplicación de la Ley de Protección de Datos Personales N° 25.326.

[1430]

Disponible al 03/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/?>

[qid=1528874672298&uri=CELEX%3A32016R0679.](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)1431_01_EN.pdf)

[1431]

Se sigue la exposición de Michèle Fink, *Blockchains and Data Protection in the European Union*, disponible al 03/05/2020 en <https://edpl.lexxion.eu/article/edpl/2018/1/6>, y su estudio titulado *Blockchain and the General Data Protection Regulation: can distributed ledgers be squared with European data protection law?* Disponible en la misma fecha en [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)1432_01_EN.pdf)

[1432]

Confr. Michèle Fink, *Blockchains and Data Protection in the European Union...* o.c. p. 17.

[1433]

Idem, p. 20.

[1434]

Idem, p. 18. Señala Fink que: “*It is important to note that the precise meaning of data portability and sovereignty, in the GDPR and elsewhere, remains unsettled. This is an important point as there are as of yet no solutions that would provide data subjects with **total control over their data**, just those that provide **more control compared to the current status quo**. Many predict that DLTs can be fashioned so that only the user has access to the public and private key, deciding freely as to when she reveals her data with external parties. Unlike ID cards or conventional medical records, **blockchains promise selective data sharing through adequate applications, ensuring privacy and reducing the risk of identity theft. Blockchains could thus facilitate new forms of identity management** by enabling individuals ‘to control access to their identity information and to create, manage and use a self-sovereign identity’.* Whether this will be the case, however, remains to be seen.” Afirma Fink: “*It is here where **law, technology and innovation must meet** and where dialogue between innovators and regulators must occur to ensure that innovation can occur, yet in a fashion that is desirable for the public good. **Much will thus depend on blockchains’ design, which must reflect technological requirements as well as public policy considerations.***” Los resaltados son míos.

[1435]

Idem, p. 21. Señala Fink que “*An ‘identifiable person’ is defined as a natural person that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.*

Where data is rendered completely anonymous, it no longer amounts to personal data and thus falls outside the scope of the legal framework.” Afirma Fichk que “*Where data is rendered pseudonymous, however, it continues to qualify as personal data as the indirect identification of a natural personal by an identifier remains possible. Two sets of data stored on blockchains can potentially be defined as personal data for the purposes of the GDPR; transactional data stored in the blocks as well as*

public keys.” Sin embargo, señala Finck que “*it is imaginable that over time, some cryptographic processes such as SHA-256 or its SHA-3 successor will be declared capable of anonymising data by courts or the European Data Protection Supervisor. Second, a number of technical solutions are currently being developed that may prevent transactional data from being directly stored on the blockchain. Buterin considers cryptographically secure obfuscation as the ‘holy grail’ of privacy on blockchains but concedes that the tool is not sufficiently developed to be used. While this solution remains unavailable, others can more readily be deployed. First, personal data could be stored off-chain and merely linked to the blockchain through a hash pointer. In such a scenario, personal data is recorded in a referenced encrypted and modifiable database and not on the blockchain.*” El resaltado es mío.

[1436]

Idem, p. 24. Afirma Fink que “*A public key is data that ‘can no longer be attributed to a specific data subject’ unless it is matched with ‘additional information’ such as a name or an address. Where these two sets of information are combined, identification is plausible, explaining why public keys cannot qualify as anonymous data. We have already seen that for data to qualify as being anonymous identification must be irreversibly prevented. Practice reveals that this cannot be said to be the case in relation to public keys. Law enforcement agencies have moreover long developed forensic chain analysis techniques to identify suspected criminals on the basis of their public keys, and a range of professional service providers performing related services have emerged. Academic research has moreover shown that public keys can be traced back to IP addresses, aiding identification. What is more, where a user transmits a transaction to the network, they usually connect directly to the network and reveal their IP address. The GDPR leaves no doubt that personal data that has ‘undergone pseudonymisation, which could be attributed to a natural person by the use of additional information’ qualifies as personal data.*

The CJEU’s adjudicative practice reinforces our conclusion that public keys qualify as personal data. In Patrick Breyer v Germany it classified dynamic IP addresses as personal data. The Court ruled that IP addresses assigned to a computing device when connected to a network may constitute personal data even if a third party (such as an internet service provider) holds the data relevant to identify an individual. This situation is in many ways analogous to the information exchanges or other service providers that are legally obliged to collect data under KYC and AML requirements”. Los resaltados son míos.

[1437]

Idem, p. 22.

[1438]

Idem, p. 29. Indica Fink que “*While it seems that, in principle, the right to modification cannot be implemented on blockchains, the provision explicitly provides that the principle of amendment must be applied with regard to the specific technology at stake. The ‘purposes of the processing’ must be accounted for and data can be rectified*

'by means of providing a supplementary statement'. This leaves us to wonder whether the addition of new data to the chain of blocks, which rectifies data previously added (without however deleting the original entry) could be considered to comply with the requirements of Article 16 GDPR. This solution could be easily applied to an append-only ledger, yet does not lead to the modification of the problematic data itself. A more suitable solution would be to store transactional data off-chain, so that it can be modified in line with data protection requirements without the need to touch the blockchain itself. Off-chain storage can again facilitate GDPR compliance in relation to transactional data but not public keys.'

[\[1439\]](#)

Idem, p. 30. Precisa Fink que los “controllers are obliged to delete personal data subject to a number of conditions, such as (i) that personal data is no longer necessary for the purposes it was collected or otherwise processed; (ii) **that the data subject withdraws consent on which the processing is based or where there is no other ground for processing;** (iii) **that the data subject objects to the processing and that there are no overriding legitimate grounds for processing;** that (iv) data has been unlawfully processed; (v) that personal data has to be erased for compliance with national or supranational law to which the controller is subject; or that (vi) personal data has been collected in relation to the offer of an information society service to a child under 16 years of age.” También puntualiza Fink que “Article 17(2) GDPR rather provides that when faced with a request for erasure, the data controller shall take **'account of available technology and the cost of implementation'** and then take 'reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data'. Here, the question arises as to whether the reference to 'available technology' could lead to an interpretation of the GDPR that dispenses from outright erasure in light of blockchains' technical limitations in favour of an alternative solution. Some have moreover suggested that formalised procedures of transmitting a key to the data subject or deleting the private key in a supervised setting could amount to erasure for the purposes of the GDPR. Unlike outright erasure, the encrypted data would still exist on-chain but could only be accessed by the data subject (through her exclusive control of the private key) or simply no longer be accessed at all. Pruning can be used to delete obsolete transactions in older blocks that are no longer necessary for the continuation of the chain but the idea remains controversial.” Con relación a los hard forks, afirma: “It should be stressed that **hard forks, which can be used to mutate blockchains in very exceptional cases, are not viable GDPR compliance-tools.** Hard forks only make sense for the most recently mined block as all subsequent blocks are rendered invalid so that all the transactions stored in these blocks would have to be reprocessed, which would be too costly regardless of the consensus protocol that is used and take a very long time (equal to the time that has passed since the block was mined, assuming equal mining power).

[1440] Idem, p. 31, nota 125.

[1441] Se siguen, en esta disgresión, mis apuntes tomados durante las clases dictadas en 2019 en el marco del Programa Fintech de ESADE BUSINESS & LAW SCHOOL, con el Prof. Marc Torrens. Cualquier error o inconsistencia, es de mi exclusiva autoría.

[1442] Confr. <https://www.statista.com/chart/17723/the-data-created-last-year-is-equal-to/> recuperado el 18/05/2020.

[1443] Confr. <https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/el-verdadero-padre-de-la-inteligencia-artificial/> recuperado el 18/05/2020.

[1444] Confr. <https://web.media.mit.edu/~minsky/papers/steps.html> recuperado el 18/05/2020.

[1445] Confr. <https://time.com/3614349/artificial-intelligence-singularity-stephen-hawking-elon-musk/> recuperado el 18/05/2020.

[1446] Confr. <https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045> recuperado el 18/05/2020.

[1447] Confr. <https://www.dailymail.co.uk/sciencetech/article-3935076/The-end-silicone-IBM-creating-carbon-chips-make-computers-TEN-times-faster.html> recuperado el 17/05/2020.

[1448] Confr. <https://www.sciencedirect.com/topics/computer-science/supervised-learning> recuperado el 18/05/2020.

[1449] Confr. <https://towardsdatascience.com/unsupervised-learning-and-data-clustering-eeecb78b422a> recuperado el 18/05/2020.

[1450] Confr. <https://stackoverflow.com/questions/6164629/what-is-the-difference-between-bottom-up-and-top-down> recuperado el 18/05/2020.

[1451] Confr. <https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/#2d1648347c9e> y en <https://hackernoon.com/explainable-ai-wont-deliver-here-s-why-6738f54216be> recuperados el 18/05/2020.

[1452] Confr. <https://givingcompass.org/article/why-businesses-fail-at-machine-learning/> recuperado el 18/05/2020.

[1453] Confr. <https://medium.com/all-things-venture-capital/ai-explainability-why-we-need-it-how-it-works-and-whos-winning-b4ca3c26b2a6> recuperado el

18/05/2020.

[1454]

Ampliar en <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>, y en el interesante artículo de Lisa Rice y Deidre Swesnik, *Discriminatory effects of credit scoring on communities of color*, en https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2014/01/Rice-Swesnik_Lead.pdf, disponibles al 18/05/2020.

[1455]

Confr. <https://towardsdatascience.com/feature-engineering-for-machine-learning-3a5e293a5114> recuperado el 18/05/2020.

[1456]

Véase <https://www.kaggle.com>

[1457]

Confr. https://threatvector.cylance.com/en_us/home/strategies-for-sanity-checking-machine-learning-models.html recuperado el 18/05/2020.

[1458]

Confr. <https://towardsdatascience.com/selecting-the-best-machine-learning-algorithm-for-your-regression-problem-20c330bad4ef> recuperado el 18/05/2020.

[1459]

Confr. <https://www.sciencedirect.com/topics/engineering/classification-algorithm> recuperado el 28/05/2020.

[1460]

Confr. <https://towardsdatascience.com/https-medium-com-chayankathuria-regression-why-mean-square-error-a8cad2a1c96f> recuperado el 18/05/2020.

[1461]

Confr. <https://www.datarobot.com/wiki/unsupervised-machine-learning/> recuperado el 18/05/2020.

[1462]

Ampliar en <https://plato.stanford.edu/entries/ethics-ai/>, recuperado el 17/05/2020.

[1463]

Confr. <https://www.forbes.com/sites/cognitiveworld/2020/02/07/biased-algorithms/#756bacc776fc> recuperado el 18/05/2020.

[1464]

Véase [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU\(2019\)0010_en.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)0010_en.pdf) recuperado el 18/05/2020.

[1465]

Confr. <https://www.criptonoticias.com/gobierno/regulacion/autoridades-argentinas-regulacion-inteligente-criptomonedas/> y en https://www.cronista.com/finanzasmercados/Reuniones-entre-el-sector-bitcoin-local-y-la-UIF-para-disenar-una-regulacion-20190405-0057.html?utm_medium=Social&utm_source=Twitter#Echobox=1554727440 disponibles al 05/05/2020.

[1466] Confr. <https://www.economista.com.ar/2019-09-criptoactivos-ha-llegado-la-hora-de-su-regulacion/> disponible al 05/05/2020. Ampliar también en <https://www.telam.com.ar/notas/201906/364815-estudiantes-de-14-universidades-del-pais-actuaron-como-legisladores-para-regular-las-criptomonedas.html>.

[1467] Confr. European Union Blockchain Observatory and Forum, *Legal and regulatory framework of blockchains and smart contracts...* o.c. p. 22.

[1468] Véase su regulación en el Código Civil y Comercial, Libro III, Título II, Capítulo XII, Arts. 1073 a 1075.

[1469] Confr. Andrés Sánchez Herrero, *Contratos celebrados por adhesión a cláusulas generales predispuestas*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo IV, Buenos Aires, 2016, p. 566. Señala Sánchez Herrero que la finalidad económica común, que preexiste, es la que determina que a su vez exista una relación de conexidad con efectos propios, existiendo una *especie de causa fin del grupo de contratos*, que excede a la causa fin de cada contrato coligado. Además, existe entre los contratos coligados una relación instrumental.

[1470] Idem, p. 572.

[1471] Idem, p. 573.

[1472] Art. 40, Ley N° 24.240. “Si el daño al consumidor resulta del vicio o riesgo de la cosa o de la prestación del servicio, responderán *el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio*. El transportista responderá por los daños ocasionados a la cosa con motivo o en ocasión del servicio. La responsabilidad es solidaria, sin perjuicio de las acciones de repetición que correspondan. Sólo se liberará total o parcialmente quien demuestre que la causa del daño le ha sido ajena.” El resaltado es mío.

[1473] Art. 1, Ley N° 25.065. “Se entiende por *sistema de Tarjeta de Crédito al conjunto complejo y sistematizado de contratos individuales cuya finalidad es:*

a) Posibilitar al usuario efectuar operaciones de compra o locación de bienes o servicios u obras, obtener préstamos y anticipos de dinero del sistema, en los comercios e instituciones adheridos.

b) Diferir para el titular responsable el pago o las devoluciones a fecha pactada o financiarlo conforme alguna de las modalidades establecidas en el contrato.

c) Abonar a los proveedores de bienes o servicios los consumos del usuario en los términos pactados.”

El resaltado es mío.

[1474] Idem, p. 578.

[1475] Idem, p. 579.

[1476] Idem, p. 581.

[1477] Idem, p. 587.

[1478] Idem, p. 589.

[1479] Idem, p. 594. Sostiene Sánchez Herrero que la ley no establece en el Art. 1075 CCCN ninguna restricción en cuanto al modo extintivo de alguno de los contratos conexos. El contrato conexo puede haberse extinguido por cumplimiento de una condición resolutoria, imposibilidad de cumplimiento, resolución por incumplimiento, o cualquier otro modo, incluyendo la frustración de la finalidad económica propia de ese contrato en particular, y la nulidad contractual.

[1480] Idem, p. 597.

[1481] Idem, p. 598. La extinción potencial de todos los demás contratos conexos, o de alguno, o de algunos, es la consecuencia de la frustración de la finalidad económica común conexas por extinción de alguno de los contratos conexos, pero respetándose el principio de conservación, lo que implica que, en caso de duda, los contratos deben mantenerse vigentes.

[1482] Idem, p. 596. Justifica su pensar así: “*admitir en este caso el efecto expansivo invocando el argumento a fortiori sería lo mismo que decir que, si alguien tiene derecho a comprar un bien por dos mil pesos, también tiene derecho a comprarlo por mil.*”

[1483] Idem, p. 602.

[1484] Art. 44, Ley N° 25.065. “Incumplimiento del proveedor. El incumplimiento de cualquiera de las obligaciones del proveedor con el titular, dará derecho al emisor a resolver su vinculación contractual con el proveedor.”

[1485] Idem, p. 606.

[1486] Idem, p. 610.

[1487] Idem, p. 585.

Art. 1120, CCCN.- “Situación jurídica abusiva. Se considera que existe una situación jurídica abusiva cuando el mismo resultado se alcanza a través de la predisposición de una pluralidad de actos jurídicos conexos.”

[1488] Confr. Art. 1251, CCCN.- “Definición. Hay contrato de obra o de servicios

cuando una persona, según el caso el contratista o el prestador de servicios, actuando independientemente, se obliga a favor de otra, llamada comitente, *a realizar una obra material o intelectual* o a proveer un servicio mediante una retribución. El contrato es gratuito si las partes así lo pactan o cuando por las circunstancias del caso puede presumirse la intención de beneficiar.” El resaltado es mío.

[1489]

Lo normal será que el contrato sea oneroso, y el comitente pague al contratista una contraprestación determinada en el contrato. Las partes son libres de pactar la forma que quieran para pagar por el desarrollo. Ahora bien, el Art. 1255 estipula sobre el particular:

“Precio. El precio se determina por el contrato, la ley, los usos o, en su defecto, por decisión judicial.

Las leyes arancelarias no pueden cercenar la facultad de las partes de determinar el precio de las obras o de los servicios. Cuando dicho precio debe ser establecido judicialmente sobre la base de la aplicación de dichas leyes, su determinación debe adecuarse a la labor cumplida por el prestador. Si la aplicación estricta de los aranceles locales conduce a una evidente e injustificada desproporción entre la retribución resultante y la importancia de la labor cumplida, el juez puede fijar equitativamente la retribución.

Si la obra o el servicio se ha contratado por un precio global o por una unidad de medida, ninguna de las partes puede pretender la modificación del precio total o de la unidad de medida, respectivamente, con fundamento en que la obra, el servicio o la unidad exige menos o más trabajo o que su costo es menor o mayor al previsto, excepto lo dispuesto en el artículo 1091.”

En materia de software, sin embargo, es más frecuente la contratación bajo modalidad *time & material*, que sería equivalente, *mutatis mutandis*, al coste y costas previsto en el Art. 1262, CCCN.- *“Sistemas de contratación. La obra puede ser contratada por ajuste alzado, también denominado “retribución global”, por unidad de medida, **por coste y costas o por cualquier otro sistema convenido por las partes**. La contratación puede hacerse con o sin provisión de materiales por el comitente. Si se trata de inmuebles, la obra puede realizarse en terreno del comitente o de un tercero. Si nada se convino ni surge de los usos, se presume, excepto prueba en contrario, que la obra fue contratada por ajuste alzado y que es el contratista quien provee los materiales.”*

Art. 1263, CCCN.- *“Retribución. Si la obra se contrata por el sistema de ejecución a coste y costas, la retribución se determina sobre el valor de los materiales, de la mano de obra y de otros gastos directos o indirectos.”* Afirma Calderón, o.c., p. 261, que en la modalidad de coste y costas el precio no se determina de antemano, sino que resulta de lo que efectivamente termine costando la obra a su finalización, en función del valor de los materiales, la mano de obra y otros gastos directos e indirectos, sobre los cuales se aplica un porcentaje pre-determinado por las partes, que es la ganancia del contratista.

[1490] Confr. Maximiliano Rafael Calderón, *Contrato de obra y servicios*, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo V, Buenos Aires, 2016, p. 225.

[1491] Idem, p. 242. Señala Calderón que dentro de las obras inmateriales se incluyen las obras literarias, científicas y artísticas referidas por el Art. 1, Ley 11.723, comprensivas de los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto y las compilaciones de datos o de otros materiales.

[1492] La cuestión puede ser distinta si se contrata a un programador, que actúa por cuenta propia, si su actividad profesional fuera considerada una profesión liberal, como es el caso del abogado –cuando se le encarga un contrato–, o del arquitecto o del ingeniero –cuando se le encarga un plano o una mensura–. Ahora bien, existen muchos programadores autodidactas que dificultan el encuadre del caso. Asumiendo que un programador de software pueda ser considerado un profesional liberal, entonces podría invocarse la aplicación del Art. 1768, CCCN: “*Profesionales liberales. La actividad del profesional liberal está sujeta a las reglas de las obligaciones de hacer. La responsabilidad es subjetiva, excepto que se haya comprometido un resultado concreto. Cuando la obligación de hacer se preste con cosas, la responsabilidad no está comprendida en la Sección 7a, de este Capítulo, excepto que causen un daño derivado de su vicio. La actividad del profesional liberal no está comprendida en la responsabilidad por actividades riesgosas previstas en el artículo 1757.*” Los resaltados son míos.

[1493] Idem, p. 226.

[1494] Idem, p. 227.

[1495] *In re* "Systemscorp S.A. c/ Redwells S.A. s/ ordinario", fallado por la Cámara Nacional de Apelaciones en lo Comercial, Sala DA, 11/08/2009. En igual sentido, véase el fallo de la Sala B, de fecha 16/9/88 en autos “De Ambrosi Lameka S.A. c/ Centro de Computación de Datos S.A.C.O.M.A.”

[1496] Confr. Quantstamp Labs, *What is a smart contract audit?* Recuperado el 08/05/2020 en <https://quantstamp.com/blog/what-is-a-smart-contract-audit>

[1497] Confr. Jan Nelson, *What is a software architect, anyway?* Recuperado el 05/05/2020 en <https://medium.com/hitachisolutions-braintrust/what-is-a-software-architect-anyway-b935ecb64c4d>

[1498] Ibid.

[1499] Ibid.

[1500] Confr. Art. 1264, CCCN.- *“Variaciones del proyecto convenido. Cualquiera sea el sistema de contratación, el contratista no puede variar el proyecto ya aceptado sin autorización escrita del comitente, excepto que las modificaciones sean necesarias para ejecutar la obra conforme a las reglas del arte y no hubiesen podido ser previstas al momento de la contratación; la necesidad de tales modificaciones debe ser comunicada inmediatamente al comitente con indicación de su costo estimado. Si las variaciones implican un **aumento superior a la quinta parte del precio pactado**, el comitente puede extinguirlo comunicando su decisión dentro del plazo de diez días de haber conocido la necesidad de la modificación y su costo estimado.*

El comitente puede introducir variantes al proyecto siempre que no impliquen cambiar sustancialmente la naturaleza de la obra.” El resaltado es mío.

[1501] *In re “JNC Proyectos y Sistemas SA c/ Banco de la Nación Argentina s/incumplimiento de contrato”, fallado por la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala II, el 11/11/2016 se definió al código fuente como “un conjunto de líneas de texto, que son las instrucciones que debe seguir la computadora para ejecutar dicho programa y describe le funcionamiento del programa respectivo. Es elaborado por un programador en algún lenguaje de programación, pero en este primer estado no es directamente ejecutable por la computadora sino que debe ser traducido a otro lenguaje (el lenguaje máquina o código objeto) que sí puede ser ejecutado por el hardware (o soporte físico) de la computadora. Para esta traducción se usan los llamados compiladores, ensambladores, intérpretes y otros sistemas de traducción. Es decir que los programadores escriben el software utilizando lenguajes de programación. Para que este código pueda ser interpretado por el ordenador o computadora es necesario “traducirlo” al lenguaje propio de las máquinas. Para esta traducción se necesitan compiladores, intérpretes u otros sistemas de traducción, que convierten el código fuente inicial en código objeto.”*

[1502] Confr. Art. 4, Ley 11.723. *“Son titulares del derecho de propiedad intelectual:*

- a) El autor de la obra;*
- b) Sus herederos o derechohabientes;*
- c) Los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.*
- d) Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, **salvo estipulación en contrario.**”* El agregado es mío. Una empresa de software puede, en casos puntuales y con determinados programadores –generalmente con los de mayor *seniority*–, acordar que ellos también sean incluidos, como personas físicas, como titulares de la propiedad intelectual en la

cual han trabajado. Lo normal, sin embargo, será que la empleadora sea inscripta como titular del derecho de propiedad intelectual, con exclusividad para lucrar con la comercialización de la misma vía contratos de licenciamiento.

[1503]

Confr. Ley N° 11.723, Art. 55 bis: “*La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción.*”

[1504]

El derecho a usar un software, conferido mediante un contrato de licencia, es una modalidad muy usual, sino la más usual, de comercializar este tipo de creaciones intelectuales. Ahora bien, el uso del licenciatarario no afecta el derecho de propiedad del licenciante, y por ello, ciertas restricciones suelen pactarse con el fin de resguardar tal propiedad. Lo contrario ocurre en el software open source.

En este sentido, *in re* “JNC Proyectos y Sistemas SA c/ Banco de la Nación Argentina s/incumplimiento de contrato”, fallado por la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala II, el 11/11/2016, se precisó, con relación al software open source: “*La Free Software Definition afirma que el “software libre” se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Por “libertad” debemos entender la situación jurídica en que se encuentra uno cuando no le alcanza ninguna prohibición, no confundiendo el término con el concepto de “gratuidad” toda vez que el software libre no significa “software no comercial” entre las libertades propias del software libre encontramos las siguientes, que deben encontrarse indefectiblemente y en forma acumulativa a) La libertad de usar el programa, con cualquier propósito (libertad 0); b) La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto; c) La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2); d) La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie (libertad 3). El acceso al código fuente es un requisito previo para esto. Para que estas libertades tengan sentido y se mantengan en el tiempo, es necesario que se cumplan dos condiciones: a) que se pueda acceder al código fuente del programa b) que ellas sean irrevocables mientras el usuario no haga nada incorrecto, como violar los términos de la licencia. (ob. Cit. pag. 461). La Open Source Definition, establece diez criterios que debe cumplir una licencia para ser considerada open source, aclarando que “fuente abierta no significa solamente acceso al código fuente sino que se deben cumplir con los siguientes criterios: a) Libre redistribución: la licencia no debe impedir a nadie la venta o entrega del software ni requerir derechos de autor u otros pagos por tal venta; b) Código fuente: el programa debe incluir el código fuente, y la licencia permitir la distribución del programa tanto en su versión fuente como en su forma compilada; c) Obras derivadas: la licencia debe permitir la realización de modificaciones u obras derivadas y su distribución bajo los mismos términos de la licencia original; d) Integridad del código*”

f) *f) No discriminación contra campos de aplicación: la licencia no puede, por ejemplo, impedir el uso del programa en negocios; g) Distribución de la licencia: las facultades concedidas deben ser aplicadas a todas las personas a quienes se redistribuya el programa, sin necesidad de obtener una licencia adicional; h) No especificidad de la licencia con relación a un producto: los derechos aplicados a un programa no deben depender de la distribución particular de software de la que forma parte; i) No restricción de la licencia con relación a otro software: la licencia no debe imponer restricciones sobre otro software que es distribuido junto con el licenciado. Por ejemplo, la licencia no debe insistir en que todos los demás programas distribuidos en el mismo medio deben ser software de fuente abierta; j) Neutralidad tecnológica de la licencia: ninguna de sus estipulaciones puede estar basada en un tipo de tecnología determinado o estilo de interfaz. En la medida en que la licencia de un software determinado satisfaga los criterios mencionados, la OSI certificará dicho cumplimiento mediante una marca certificada: la "OSI Certified" (390). Dada la proliferación de productos y licencias en el mercado, la existencia de este certificado proporciona a la comunidad una forma confiable de saber si un software es realmente open source y de esta forma tener cierta previsibilidad acerca de lo que puede y no puede hacer con el mismo.*" En el fallo citado se dijo también: "en todos los casos las licencias determinan expresamente las facultades del usuario en cuanto a los límites en el uso de las aplicaciones y programas. Es decir que el usuario sólo tiene permitido aquello que surge expresamente del contenido del acuerdo de licencia. En virtud de las libertades que confieren, las licencias utilizadas para distribuir el software pueden clasificarse en "libres" y "propietarias", siendo la primera de ellas la única que permite al usuario ejecutar el programa en tantas computadoras como desee, estudiarlo, adaptarlo, distribuirlo, mejorarlo y publicarlo. Dentro de las licencias libres, encontramos algunas que tienen por finalidad perpetuar la libertad y evitar que se añadan nuevas restricciones, para lo cual insertan la cláusula copyleft. Contrariamente a lo que se supone, el copyleft no se opone al copyright. Antes bien, se nutre de él y le da un nuevo significado, preservando el carácter de libre del Software. De esta forma, el software libre goza de una doble protección: a través de la licencia se imponen determinadas restricciones contractuales que otorgan permiso legal para copiar, distribuir y/ o modificar el software. Mediante la ley de copyright se permite que esa licencia sea válida y obligatoria."

Así, salvo que la licencia disponga lo contrario, normalmente el uso licenciatario no permitirá al licenciatario modificar el código fuente sin una expresa cláusula contractual en tal sentido, ya que "la provisión del programa fuente no implica

necesariamente la facultad de modificarlo, en tanto y en cuanto esta última no se encuentre expresamente pactada en el contrato. A la pregunta que formula la quejosa referida a para qué otro motivo si no es la modificación la demandada otorgaría los códigos fuentes del programa cabe responder que le otorga además de estabilidad, seguridad. Como señalara, el programa fuente requiere de una compilación para que pueda ser interpretado y ejecutado por la máquina, poseer los códigos fuente del programa otorga independencia en cuanto al mantenimiento, si por algún agente externo que puede ser un virus, una inundación o un incendio se vieran afectados los archivos ejecutables y compilados, teniendo el código fuente, los mismos se pueden volver a compilar y generar pudiendo así continuar con el trabajo habitual y sin que ello implique modificación del programa en forma alguna.” A falta de una cláusula expresa en tal sentido, el licenciatarario que modifique el código fuente se pondrá en situación de “incumplimiento del contrato de Licenciamiento de Software y Prestación de Servicios, por uso indebido de software, violación de confidencialidad, utilización en una máquina diferente a la asignada, copias no autorizadas de software, alteraciones y/o modificaciones del programa así como también del código fuente.”

[1505]

In re “MICROSOFT CORPORATION C/ AREA 099 S. A. S/ DAÑOS Y PERJUICIOS”, de la Cámara Nacional de Apelaciones en lo Civil, Sala G, el 12/02/2019.

[1506]

Ibid.

[1507]

Ibid.

[1508]

Ibid.

[1509]

Ibid.

[1510]

Idem, p. 263.

[1511]

Ibid. Art. 1272, CCCN.- Plazos de garantía. Si se conviene o es de uso un plazo de garantía para que el comitente verifique la obra o compruebe su funcionamiento, la recepción se considera provisional y no hace presumir la aceptación.

Si se trata de vicios que no afectan la solidez ni hacen la obra impropia para su destino, no se pactó un plazo de garantía ni es de uso otorgarlo, aceptada la obra, el contratista: (a) queda libre de responsabilidad por los vicios aparentes; y (b) responde de los vicios o defectos no ostensibles al momento de la recepción, con la extensión y en los plazos previstos para la garantía por vicios ocultos prevista en los artículos 1054 y concordantes.” [1] [SEP]

[1512]

Idem, p. 264.

[1513]

Confr. CCCN, Art. 2: “La ley debe ser interpretada teniendo en cuenta sus

palabras, sus finalidades, las leyes análogas, las disposiciones que surgen de los tratados sobre derechos humanos, los principios y los valores jurídicos, de modo coherente con todo el ordenamiento.”

[1514] Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction to smart contracts...o.c.*, p. 19.

[1515] Véase *supra* en § 2.4.2.

[1516] Confr. Zikai Alex Wen y Andrew Miller, *Scanning live Ethereum contracts for “Unchecked-Send” bug*, disponible al 05/05/2020 en <https://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/>.

[1517] *Ibid.*

[1518] Véase, por ejemplo, las 24 buenas prácticas y los 5 manuales publicados sobre errores comunes de programación, ya conocidos y resueltos, en relación a Ethereum y su lenguaje Solidity, disponibles al 08/05/2020 en <https://github.com/ConsenSys/smart-contract-best-practices/blob/master/docs/bibliography.md>. Véase también, en GitHub, *Ethereum Smart Contract Best Practices*, en https://consensys.github.io/smart-contract-best-practices/security_tools/, disponible al 08/05/2020, donde se presentan herramientas de visualización, de análisis estático y dinámico, casos ya conocidos, y en general, las distintas herramientas de programación utilizadas para detectar código sospechoso, confuso o incompatible entre distintas arquitecturas en programas, i.e., errores de programación que escapan al habitual análisis sintáctico que hace el compilador. Se denominan herramientas de tipo *lint* y generalmente funcionan realizando un análisis estático del código fuente.

Las construcciones sospechosas que se suelen buscar son usos de variables antes de ser inicializadas o creadas, condiciones que no varían bajo ninguna circunstancia (Son siempre verdaderas o siempre falsas) y cálculos cuyos resultados probablemente caigan fuera del rango permitido por las variables utilizadas. En los compiladores optimizados (cuya principal motivación es la generación de código de alta calidad) también se pueden encontrar muchos de los análisis habitualmente realizados por *lint*. También se está empezando a incluir la detección de estas construcciones incorrectas en su lista de avisos (*Warnings*).

Las sucesivas generaciones de herramientas del estilo de *lint* han seguido ampliando en rango de construcciones incorrectas o sospechosas. Las herramientas más avanzadas realizan cada vez más comprobaciones, como por ejemplo, que el código sea consistente entre distintos compiladores, o el soporte para incorporar anotaciones acerca del comportamiento esperado o las propiedades del código.

[1519] Confr. Samuel Bourque y Sara Fung Ling Tsui, *A lawyer's introduction to smart contracts...o.c.*, p. 17.

[1520] Véase <https://www.openlaw.io>

[1521] Véase <https://clause.io>

[1522] Véase <http://www.commonaccord.org>

[1523] Véase <https://blog.agrello.org/tagged/smart-contracts>

[1524] Véase <https://legalese.com>

[1525] Véase *supra* en § 2.4.3, 2.4.4 y 2.8.

[1526] Confr. Firas Al Khalil, Marcello Ceci, Leona O'Brien y Tom Butler, *A solution for the problems of translation and transparency in smart contracts*, disponible al 06/05/2020 en <https://e9a5d5c6.stackpathcdn.com/wp-content/uploads/2017/06/GR3C-Smart-Contracts-White-Paper-2017.pdf>, p. 6.

[1527] Ibid.

[1528] Idem, p. 9.

[1529] Idem, p. 10.

[1530] Confr. Amy Castor, *One of Ethereum's earliest smart contract languages is headed for retirement*, disponible al 05/05/2020 en <https://www.coindesk.com/one-of-ethereums-earliest-smart-contract-languages-is-headed-for-retirement>. Puede ampliarse en Manuel Aráoz, *Serpent Compiler Audit*, disponible en la misma fecha en https://docs.google.com/document/d/1_PqXuAkvqUAOG3jbBvaUvqN6W90eJ3N4Id7

[1531] Confr. <https://choosealicense.com/licenses/mit/>. Véase *infra* en § 4.7.5.

[1532] Confr. Pablo Palazzi, *Orientaciones jurisprudenciales en materia de contratos informáticos: obligaciones de resultado, validez de cláusulas de limitación de responsabilidad y naturaleza jurídica de la licencia de software*, en Revista Derecho y Nuevas Tecnologías, N° 1, CeTyS, 2017, p. 145.

[1533] *In re* C. Nac. Com., sala D, 13/5/2008, Argentoil S.A. vs. Soft Pack S.A., ED 7/10/2008, LA LEY 2008-D, 367.

[1534] *In re* CNCom, Sala C, 10/10/2008, A&CISA c/Buenos Aires Software.

[1535] *In re* CNCom, Sala D, 16/3/2009, Coca Cola Polar Argentina S.A vs. Soft

Center S.A.

[1536]

Cámara Nacional de Apelaciones en lo Comercial, sala A, 30/04/2015, Zival' S S.A. c. Samia, Marcelo Fabián s/ ordinario. La actora contrató a la demandada para la elaboración y desarrollo de un software informático a medida denominado S.A.I. (Sistema de Administración Integral) donde los clientes con sus interfaces gráficas accederían a un servidor de aplicaciones que se conectaría con una base de datos que almacenaría la información derivada de la administración general de la empresa con sus sucursales. El programa nunca terminó de ser elaborado (tenía 25% de progreso según la pericia informática). En ambas instancias se hace lugar a la demanda por incumplimiento de lo acordado. Las cuestiones que se rescatan de este precedente son: (i) las obligaciones del proveedor de servicios informáticos son obligaciones de resultado y (ii) la responsabilidad es *objetiva*.

[1537]

Confr. Pablo Palazzi, *Orientaciones jurisprudenciales en materia de contratos informáticos: obligaciones de resultado, validez de...o.c.* p. 155, nota 13, cita el caso CCiv y Com San Isidro, Sala 1, 8/5/2008, Sociedad Escolar Alemana de Villa Ballester vs. Ditada, Nicolas M. y otro, JA 2008-IV-395 (rechazando la existencia de una relación de consumo y por ende de la aplicación de la LDC a un software a medida porque éste estaba destinado a actividades relacionadas con los servicios que prestaba la actora). En caso de ausencia de este tipo de cláusula limitativa, sostiene Palazzi, p. 156 que el proveedor no solo deberá indemnizar el valor de lo contratado sino que corresponde indemnizar *el daño a la actividad productiva de la empresa licenciada*. Este daño se compone del tiempo y valor de horas hombre propias, empleadas en la implementación del software que funcionó incorrectamente. Este tiempo podría haberse empleado en un actividad mas útil y no en la implementación del programa con errores.

Si alguna duda cabe, afirma Palazzi que en los casos de reclamos por uso no autorizado de software en empresas, los titulares de programas de ordenador no sólo reclaman el valor de la licencia *sino también el lucro ilícito obtenido por el demandado*. Este lucro ilícito demuestra que la empresa obtiene un beneficio por el uso del software. Por ende, la privación del mismo o su funcionamiento defectuoso, y el tiempo y recursos aplicados infructuosamente al mismo, son un gasto al que tiene derecho a ser indemnizado. En este sentido, cita Palazzi el fallo del JNCiv. N. 31, 9/11/2005, Microsoft Corporation v. Anselmi Gerencia de Riesgos S.A. (RCyS 2006-1094), cofirmado por CNCiv, Sala G, 28/4/2006, publicado en RRCyS, Año VIII, n. 8, agosto 2006, pag. 58.

[1538]

Confr. Pablo Palazzi, *Orientaciones jurisprudenciales en materia de contratos informáticos: obligaciones de resultado, validez...o.c.*, p. 157 afirma que lo normal es que el software se licencie, para que la propiedad quede en cabeza de su titular. Afirma Palazzi que desde hace casi cuatro décadas, en la industria del software la práctica

contractual es la de adoptar licencias. Sin esta licencia, que constituye una *autorización de uso*, el usuario no podría usar legalmente la obra, y es por ello que estas licencias conllevan limitaciones como la posibilidad de hacer una sola copia de respaldo, prohibir la ingeniería inversa, el adaptar o modificar la obra, traducirla para que funcione en otros sistemas o el no instalarla en mas ordenadores que los autorizados. Afirma Palazzi que la distinción entre compraventa y licencia tiene mucho sentido para entender que el licenciante no se desprende de la propiedad del programa (y a veces siquiera de la copia) sino que sólo autoriza su uso. También es importante en otras áreas como la impositiva o cuando se discute el agotamiento de los derechos sobre la copia adquirida por el usuario. En el caso “Soft Center” el tribunal entendió que había una locación de obra. En cambio en el caso “Buenos Aires Software” el tribunal se inclinó por entender que se trataba de una licencia. Del caso “Buenos Aires Software” esta categorización es muy relevante pues lleva al tribunal a decidir la aplicación del plazo de diez años para el reclamo, en vez del plazo de reclamo establecido para los vicios redhibitorios. La naturaleza de la licencia de software no había sido tratada por nuestros tribunales. El caso “Buenos Aires Software” es el primero que lo hace en forma expresa y la caracterización que el tribunal da a esta clase de contratos como licencia nos aparece adecuada en función de la naturaleza del objeto licenciado y la práctica comercial.

[1539]

Véase <https://openzeppelin.com>

[1540]

Véase <https://diligence.consensys.net>

[1541]

Confr. Quantstamp Labs, *What is a smart contract audit?* Recuperado el 08/05/2020 en <https://quantstamp.com/blog/what-is-a-smart-contract-audit>

[1542]

Las auditorías típicamente tienen lugar *ex post facto*, cuando el trabajo de programación ya ha sido concretado. Ahora bien, últimamente se ha postulado que, dada la creciente complejidad de los contratos inteligentes, es recomendable incluir chequeos de seguridad durante el proceso de programación, confr. <https://diligence.consensys.net/blog/2020/03/new-offering-1-day-security-reviews/>, recuperado al 08/08/2020. Allí, con razón se afirma que: “*if you’re building a house, you’d rather learn about problems in the foundation before you’ve built the rest of the house. If you learn about such problems at the very end of construction, they’re going to be extremely expensive to fix properly. There are a multitude of ways we engage with clients early, but 1-day security reviews are a particularly useful tool. Such a review is an inexpensive way to discover fundamental issues early and have a chance to resolve them before it’s time for a full audit.*”

[1543]

Véase *supra* en § 2.6.3 el análisis de *The LAO*. Al 08/05/2020, está disponible el informe final de auditoría de los smart contracts involucrados en este link:

<https://diligence.consensys.net/audits/2020/01/the-lao/>.

[1544] Confr. Ted Mlynar y Ira Schaefer, *Blockchain smart contracts need a new kind of due diligence*, recuperado el 08/05/2020 en <https://www.coindesk.com/blockchain-smart-contracts-need-new-kind-due-diligence>.

[1545] Ibid.

[1546] Ibid.

[1547] Confr. Maximiliano Rafael Calderón, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo V, Buenos Aires, 2016, p. 226.

[1548] Se aplican a los servicios los Arts. 1278, CCCN.- “*Normas aplicables. Resultan aplicables a los servicios las normas de la Sección 1a de este Capítulo y las correspondientes a las obligaciones de hacer*”; Art. 774, CCCN.- “*Prestación de un servicio. La prestación de un servicio puede consistir: (a) en realizar cierta actividad, con la diligencia apropiada, independientemente de su éxito. Las cláusulas que comprometen a los buenos oficios, o a aplicar los mejores esfuerzos están comprendidas en este inciso*”

[1549] Art. 21, Ley N° 24.240. “*Presupuesto. En los supuestos contemplados en el artículo anterior, el prestador del servicio debe extender un presupuesto que contenga como mínimo los siguientes datos:*

- a) *Nombre, domicilio y otros datos de identificación del prestador del servicio;*
- b) *La descripción del trabajo a realizar;*
- c) *Una descripción detallada de los materiales a emplear.*
- d) *Los precios de éstos y la mano de obra;*
- e) *El tiempo en que se realizará el trabajo;*
- f) *Si otorga o no garantía y en su caso, el alcance y duración de ésta;*
- g) *El plazo para la aceptación del presupuesto;*
- h) *Los números de inscripción en la Dirección General Impositiva y en el Sistema Previsional.*”

Art. 22, Ley N° 24.240. “*Supuestos no Incluidos en el Presupuesto. Todo servicio, tarea o empleo material o costo adicional, que se evidencie como necesario durante la prestación del servicio y que por su naturaleza o características no pudo ser incluido en el presupuesto original, deberá ser comunicado al consumidor antes de su realización o utilización. Queda exceptuado de esta obligación el prestador del servicio que, por la naturaleza del mismo, no pueda interrumpirlo sin afectar su calidad o sin daño para las cosas del consumidor.*”

[1550] Art. 23, Ley N° 24.240. “*Deficiencias en la Prestación del Servicio. Salvo*

previsión expresa y por escrito en contrario, si dentro de los treinta (30) días siguientes a la fecha en que concluyó el servicio se evidenciaren deficiencias o defectos en el trabajo realizado, el prestador del servicio estará obligado a corregir todas las deficiencias o defectos o a reformar o a reemplazar los materiales y productos utilizados sin costo adicional de ningún tipo para el consumidor.”

[1551] Véase *supra* en § 3.3.1.6 y 3.4.6.

[1552] Al momento en que se escribe este Manual, Abril de 2020, no existe aún en Argentina una regulación específica para los *Exchanges* de criptoactivos, pero sí existe una regulación para las billeteras digitales. La actividad, como se vió *supra* en § 3.3, está regulada en muchos países.

[1553] Véase *supra* en § 3.4.6.1.2 y 2.2.3.1.1.

[1554] Véase *supra* en nota 421 y 422. Ampliar también en <https://uk.reuters.com/article/crypto-currencies-japan-cybercrime/japans-tech-bureau-says-about-60-mln-stolen-in-crypto-hack-idUKL3N1W5692>, recuperado el 08/05/2020.

[1555] Confr. *Report from Study Group on Virtual Currency Exchange Services*, disponible al 05/05/2020 en <https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181221-1.pdf>.

[1556] *Idem*, p. 4. Sostuvieron los expertos japoneses: “*In the Study Group meeting, there is an opinion that it might be necessary to increase the minimum capital (currently 10 million JPY), which is one of the registration requirements, in order to respond to business expansion of SPs, and to decrease administrative costs for the examination of application caused by easily entering into market. On the other hand, another member states that given the possibility of innovation, the government should not apply the strict regulations equally at the entry stage but should apply regulations corresponding to the risk level. It is considered appropriate to request that the funds for reimbursement should be preserved separately from the company’s assets and customers’ assets. It is also conceivable that holding non-risk assets, such as cash, may be required as the funds for reimbursement. It is, however, necessary to take into consideration that SPs have an obligation to customers to return the virtual currency under management and that the face value of non-risk assets may become less than the required amount due to fluctuations in the virtual currency prices. Furthermore, even if virtual currency under management is leaked, the SP’s obligation to return the virtual currency to the customers is not necessarily exempted. Therefore, it would be appropriate to require SPs to hold assets in the same kind of virtual currency as the funds for reimbursement.*” Los resaltos me pertenecen.

- [1557] Véase *supra* en nota 988 e *infra* en nota 2036.
- [1558] Véase *supra* en nota 423.
- [1559] Ampliar en <https://www.bbc.com/news/world-europe-50821547>, recuperado el 08/05/2020.
- [1560] Véase <https://exchange.ripio.com/es/>
- [1561] De acuerdo a los términos y condiciones publicados al 08/05/2020 en <https://exchange.ripio.com/es/terminos/>, cláusula 3.2: “*siendo el sitio un portal orientado al intercambio y obtención de monedas digitales a través de medios de pago físicos provistos por la empresa CuentaDigital S.R.L, todos los términos y condiciones especificados en www.cuentadigital.com/downloads/CuentaDigitalContrato.pdf también aplican a los términos indicados en este contrato.*” Los términos y condiciones de uso de Cuenta Digital están disponibles, al 08/05/2020 en <http://www.cuentadigital.com/downloads/CuentaDigitalContrato.pdf>.
- [1562] Confr. *Report from Study Group on Virtual...o.c.*, p. 9.
- [1563] Confr. <https://www.amf-france.org/en/professionals/fintech/my-relations-amf/obtaining-approval-ico/black-list>, disponible al 08/05/2020.
- [1564] Confr. <https://www.finma.ch/en/finma-public/warning-list/> disponible al 08/05/2020.
- [1565] Confr. <https://www.securities.io/finma-releases-annual-report-list-security-tokens-and-dlt/> disponible al 08/05/2020.
- [1566] Confr. Fernando Branciforte, *Análisis de las comunicaciones “A” 6859 y “A” 6885 del BCRA. Su implicancia para las empresas Fintech, usuarios y consumidores de sus servicios*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.
- [1567] Ibid.
- [1568] Art. 1345, CCCN.- Definición. Hay contrato de corretaje cuando una persona, denominada corredor, se obliga ante otra, a mediar en la negociación y conclusión de uno o varios negocios, sin tener relación de dependencia o representación con ninguna de las partes.
- [1569] Confr. Maximiliano Rafael Calderón, en *Tratado de Derecho Civil y Comercial*, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo V, Buenos Aires, 2016, p. 406. Señala Calderón que

no debe confundirse el corretaje, en tanto contrato típico y autónomo, con el uso de la palabra corretaje para referirse a cualquier actividad realizada por un corredor, ni con la regulación subjetiva de la actividad profesional del corredor, contenida en la Ley N° 20.266, Capítulo XII.

[1570]

Confr. Calderón, o.c., p. 422 sostiene que el corredor puede representar a ambas partes –vendedor y comprador– en la intermediación, sin que ello desnaturalice al contrato. En tal caso, se denomina corretaje bilateral.

[1571]

Art. 1348, CCCN.- Prohibición. Está prohibido al corredor: (a) adquirir por sí o por interpósita persona efectos cuya negociación le ha sido encargada; y (b) tener cualquier clase de participación o interés en la negociación o en los bienes comprendidos en ella. ^[L]_[SEP]

[1572]

La comisión sólo se paga si el negocio se concluye, y puede pactarse de cualquier manera, incluyendo un monto fijo, retribución en especie, o un porcentaje del negocio. Si el corredor no está inscripto en la matrícula, no tiene derecho a cobrarla. La comisión por intermediación inmobiliaria está regulada en el Art. 77 de la Ley N° 24.441. Tanto el comitente como el tercero con quien éste cierre el contrato le deben la comisión al corredor; si se trata de viviendas nuevas, sólo el comitente debe pagarla.

El Art. 1352 regula tres casos en los que la comisión se debe a pesar de vicisitudes que pueden afectar al contrato celebrado; y el Art. 1353 regula dos casos en los que la comisión no se debe en ningún caso.

[1573]

Art. 1347, CCCN.- Obligaciones del corredor. El corredor debe: (a) **asegurarse de la identidad de las personas que intervienen en los negocios en que media y de su capacidad legal para contratar**; (b) ^[L]_[SEP]proponer los negocios con exactitud, precisión y claridad, absteniéndose de mencionar supuestos inexactos que puedan inducir a error a las partes; (c) comunicar a las partes todas las circunstancias que sean de su conocimiento y que de algún modo puedan influir en la conclusión o modalidades del negocio; (d) mantener confidencialidad de todo lo que concierne a negociaciones en las que interviene, la que sólo debe ceder ante requerimiento judicial o de autoridad pública competente; (e) asistir, en las operaciones hechas con su intervención, a la firma de los instrumentos conclusivos y a la entrega de los objetos o valores, si alguna de las partes lo requiere; (f) guardar muestras de los productos que se negocien con su intervención, mientras subsista la posibilidad de controversia sobre la calidad de lo entregado. El resaltado es mío.

[1574]

Confr. Art. 1347, CCCN, inc. c)

[1575]

Arts. 31 a 35. Podría sostenerse que la obligación de inscribirse en la matrícula

para poder actuar como corredor, sea persona humana, sea persona jurídica, es en realidad una *carga*, ya que la falta de inscripción sólo produce la falta de acción para cobrar la remuneración o retribución (Art. 33), norma que procura sancionar al corredor *de hecho*, pero en modo alguno nulifica al contrato de compraventa en el cual haya intermediado y vinculado a las partes. Afirma Calderón, o.c. p. 412, nota 10 que el anteproyecto de Código Civil y Comercial de la Nación admitía el derecho a cobro de la comisión al corredor de hecho.

[1576] En efecto, las Normas de la CNV T.O. 2013 regulan al Agente de Corretaje de Títulos Valores en su Título VII, Capítulo VI.

[1577] Por ejemplo, la Provincia de Córdoba regula específicamente el corretaje inmobiliario en la Ley N° 9445.

[1578] Confr. Yahoo Finance, *Hackers have stolen \$400 million worth of ICO investments*, recuperado el 10/05/2020 en <https://finance.yahoo.com/news/hackers-stolen-400-million-worth-194947712.html>.

[1579] Confr. https://en.wikipedia.org/wiki/Mt._Gox

[1580] Ibid.

[1581] Confr. <https://qz.com/753958/the-65-million-bitfinex-hack-shows-that-it-is-impossible-to-tell-a-good-bitcoin-company-from-a-bad-one/> recuperado el 09/05/2020.

[1582] Confr. <https://www.cnn.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html> recuperado el 09/05/2020. Véase *supra* nota 421.

[1583] Para una lista completa de todos los ciberataques a *Exchanges*, véase <https://selfkey.org/list-of-cryptocurrency-exchange-hacks/> recuperado el 09/05/2020.

[1584] Confr. <https://www.coindesk.com/upbit-is-the-sixth-major-crypto-exchange-hack-of-2019> disponible al 08/05/2020.

[1585] Véase *supra* en § 3.4.6.1.

[1586] La demanda colectiva está disponible, al 08/05/2020 en <http://cryptsyreceivership.com/v1/wp-content/uploads/2016/06/2016-2-22-DE-8-AMENDED-CLASS-ACTION-COMPLAINT.pdf>. La demanda se interpuso contra la sociedad que operaba la plataforma y sus dos directivos.

[1587] Una segunda acción colectiva fue iniciada a fines de 2016 por los mismos abogados pero contra un muy conocido *Exchange* con base en San Francisco,

CoinBase. La demanda colectiva está disponible, al 08/05/2020 en <https://www.coinbasesettlement.com> y fue trazada en Enero de 2020, confr. <https://www.law.com/dailybusinessreview/2020/01/28/coinbase-bitcoin-exchange-agrees-to-1-million-class-action-settlement/?slreturn=20200408181956> disponible al 08/05/2020. Se sostiene en la demanda que las criptomonedas “robadas” de Cryptsy fueron cambiadas en Coinbase, quién no actuó con la debida diligencia al no sospechar sobre el origen de un volumen tan grande de criptomonedas depositadas a nombre personal de un directivo de Cryptsy, Paul Vernon, que sigue prófugo y ya ha sido condenado en rebeldía. Confr. <https://news.bitcoin.com/class-action-cryptsy-coinbase/> disponible al 08/05/2020.

[1588] Véase la demanda colectiva disponible, al 08/05/2020 en <http://cryptsyreceivership.com/v1/wp-content/uploads/2016/06/2016-2-22-DE-8-AMENDED-CLASS-ACTION-COMPLAINT.pdf>

[1589] La certificación de la *class action* está disponible al 08/05/2020 en <http://cryptsyreceivership.com/v1/wp-content/uploads/2016/06/Order-Granting-Class-Certification.pdf>

[1590] Al 08/05/2020, el acuerdo transaccional preliminar está disponible en <http://cryptsyreceivership.com/v1/wp-content/uploads/2016/06/Order-Granting-Motion-for-Preliminary-Approval-of-Class-Action-Settlement-Directing-the-Issuance-of-Class-Notice-and-Scheduling-a-Final-Approval-Hearing.pdf>

[1591] Confr. <https://news.bitcoin.com/vanished-cryptsy-ceo-big-vern-ordered-to-pay-8m-in-class-action-lawsuit/> recuperado el 08/05/2020.

[1592] Véase <https://www.whitecase.com/publications/alert/cryptocurrencies-property-trust-and-mistake> disponible al 08/05/2020.

[1593] El contrato que Quoine utilizaba estaba contenido en los términos y condiciones de su web site. Confr. https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf, disponible al 08/05/2020.

[1594] Ibid.

[1595] Confr. <https://www.coindesk.com/south-korean-exchange-loses-5-million-in-accidental-bitcoin-airdrop>, recuperado el 10/05/2020.

[1596] Confr. Michel Rauchs, Apolline Blandin, Kristina Klein, Gina Pieters, Martino Recanatini, y Bryan Zhang, *2nd Global Cryptoasset Benchmarkings Study*, disponible al 10/05/2020 en

https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-09-ccaf-2nd-global-cryptoasset-benchmarking.pdf, p. 50.

[1597]

Idem, p. 49.

[1598]

Ibid.

[1599]

Confr. John Salmon y Gordon Myers, IFC, World Bank, *Blockchain and Associated Legal Issues for Emerging Markets*, disponible al 10/05/2020 en <https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cfc1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F>, p. 4.

[1600]

Confr. <https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/> recuperado el 10/05/2020 y en <https://www.ledgerinsights.com/teen-hacks-hardware-crypto-wallet/>. Ampliar en <https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/>, disponible a la misma fecha.

[1601]

Confr. <https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/>, disponible al 10/05/2020.

[1602]

El autor quiere agradecer muy especialmente la guía recibida para la redacción de este apartado por parte del Mag. en Propiedad Intelectual Dante A. Pusiol, A.P.I., quien se desempeña como docente en estos temas en los programas de incubación del CEINN-UCC, en el Curso de Posgrado en Derecho Empresarial que se dicta en la Escuela de Negocios ICDA y en la Maestría en Derecho de Empresas de la Universidad Católica de Córdoba.

[1603]

Véase *supra* en § 2.2.3.1.1.

[1604]

Véase *supra* nota 420.

[1605]

Confr. Maximiliano Rafael Calderón, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo V, Buenos Aires, 2016, p. 433.

[1606]

Idem, p. 434.

[1607]

Ibid.

[1608]

CCCN, Art. 746 y siguientes.

[1609] CCCN, Art. 762 y siguientes

[1610] Confr. Maximiliano Rafael Calderón, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director)...o.c., p. 445.

[1611] Confr. Pablo Palazzi, *Orientaciones jurisprudenciales en materia de contratos informáticos: obligaciones de resultado, validez de cláusulas de limitación de responsabilidad y naturaleza jurídica de la licencia de software*, en Revista Derecho y Nuevas Tecnologías, N° 1, CeTyS, 2017, p. 161.

[1612] Idem, p. 162.

[1613] Ibid.

[1614] Idem, p. 165. Sostiene Palazzi que la obligación de garantizar la propiedad intangible es una cláusula implícita en todo contrato relacionado con propiedad intelectual y como tal en ausencia de cláusula específica rige la garantía de evicción. Como mínimo el proveedor deberá garantizar que el software no se encuentra en infracción a las normas de derecho de autor, secretos comerciales o patentes que resulten aplicables, que no se encuentra en infracción a otras licencias, y en especial que no posee código abierto o que si lo incluye cumple con las reglas de la respectiva licencia que resulte aplicable. Esto constituye una garantía mínima que como vimos debe estar presente, pero lo ideal sería también incluir una indemnidad frente a todas estas representaciones.

[1615] Ibid, nota 42.

[1616] Confr. Darío Veltani, *El contrato de licencia de software*, publicado en en Revista Derecho y Nuevas Tecnologías, N° 1, CeTyS, 2017, p. 111.

[1617] Idem, p. 117.

[1618] Idem, p. 116. Afirma Veltani que el licenciataro o usuario es la persona que adquiere los derechos previstos en la licencia para utilizar el software en los términos que indica la licencia y, en algunos casos, las figuras de licenciataro y usuario podrían no coincidir, cuando el usuario final es un tercero autorizado por el licenciataro. Esta situación debe estar prevista en el contrato de licencia para evitar inconvenientes respecto de la eventual inoponibilidad del contrato de licencia a ese tercero.

[1619] Idem, p. 116. Afirma Veltani que el licenciante, que puede ser *per se* el desarrollador del software o una persona con derechos suficientes para otorgar la licencia.

[1620] Idem, p. 116, nota 19. En el caso “Coca Cola Polar Argentina c/ Soft Center SA”

se calificó al contrato como de obra, y no como una mera licencia.

[1621]

Idem, p. 119. Afirma Veltani con toda razón que en los primeros modelos de negocio vinculados con el software, el licenciante obtenía sus ingresos fundamentalmente por la comercialización de la licencia. El software no requería de actualizaciones constantes, y cada nueva versión implicaba una nueva licencia. En este modelo, la licencia era, por definición, perpetua. Sin embargo, este modelo se fue modificando con el tiempo, y en la actualidad la tendencia es que los ingresos del licenciante no se basen tanto en el pago de la licencia de software sino en los *servicios conexos y complementarios* que se dan en el marco de dicha licencia de software (v.g. el servicio de actualización, soporte técnico, implementación, etc.).

En este contexto, la determinación expresa del plazo y las condiciones de vigencia en la licencia aparece como una cláusula esencial. De acuerdo con el modelo de negocios aplicable, la licencia de software puede otorgarse: (i) a perpetuidad; (ii) por un plazo determinado, renovable (automáticamente o no); o (iii) por un plazo incierto o sujeto al cumplimiento de una condición (v.g. una licencia de software complementaria a una prestación principal contratada por el usuario y que se confiere mientras esté vigente dicha prestación principal). A su vez, dentro de las condiciones de vigencia pueden incluirse también obligaciones para el licenciatario, cuyo incumplimiento determine la terminación anticipada del contrato. Entre las más destacables señala Veltani: (a) la obligación de pagar el precio, del modo acordado; (b) la obligación de cumplir con las condiciones técnicas previstas en la licencia o las que indique el licenciante para el correcto funcionamiento del software licenciado; o (c) no realizar tareas de ingeniería inversa y/o modificar el código fuente del software.

[1622]

Idem, p. 120. Afirma Veltani que el contrato de licencia de software debe precisar de modo expreso y claro cuál es la contraprestación que recibirá el licenciante, de qué modo lo hará, y a qué corresponde (en caso de existir diversos tipos de contraprestaciones). Históricamente, cuando los ingresos del licenciante se basaban en la comercialización de la licencia, la determinación de la contraprestación era un tema sencillo: el licenciatario debía pagar, habitualmente por única vez al momento de adquirir la licencia, un precio determinado. Como única complejidad a destacar podía ocurrir, bajo este esquema, que dicho precio fuera distribuido en varios pagos, en cuyo caso debía preverse la eventual mora y sus consecuencias. Ahora bien, con el cambio en los esquemas de licenciamiento, la cuestión de la contraprestación también se vio modificada. En efecto, la cláusula relativa a la contraprestación debe considerar alternativas diferenciales tales como el pago por: (i) el uso del software; (ii) la prestación de servicios de soporte; y (iii) la prestación de servicios complementarios, como por ejemplo el almacenamiento de información o servicios de seguridad. En el caso de la contraprestación por el uso del software, podría establecerse un pago único - como en el esquema de licenciamiento histórico- que permita la utilización del

software a perpetuidad o por un cierto tiempo, o bien la obligación de realizar el pago con cierta periodicidad, de modo tal que la vigencia de la licencia esté sujeta a ese pago periódico

Afirma Veltani que respecto de la contraprestación por servicios de soporte, la cuestión es algo más compleja, dado que habitualmente este tipo de servicios se presta tomando en cuenta las horas trabajadas. Por lo tanto, la cláusula debería prever, como mínimo: (a) quién prestará el soporte (podría ser el licenciante o un tercero); (b) el tipo de soporte que se prestará (puede ser preventivo, correctivo, o de ambos tipos); (c) la tasa horaria que cobrará el licenciante o el tercero autorizado a prestar el soporte y cómo se determinarán las horas de soporte prestadas; y (d) el mecanismo de información de las horas de soporte y su aceptación por parte del licenciario. Por último, con relación a la prestación de servicios complementarios, la contraprestación dependerá del tipo de servicio de que se trate, pero es aconsejable que sea expresa y que se refiera a parámetros que puedan ser verificados objetivamente. Si el servicio complementario fuera el almacenamiento de información, la cláusula que regule la contraprestación por dicho servicio debería establecer claramente cuál sería el precio por el espacio de almacenamiento contratado por un tiempo determinado.

[1623]

Idem, p. 121. Afirma Veltani es conveniente que la licencia describa las funcionalidades del software licenciado, siendo habitual que se incluyan cláusulas que indican que el licenciante no otorga garantía alguna de que el software sirva para un propósito determinado, situación muy perjudicial para los intereses de ambas partes del contrato, y que debe ser evitada. Si el contrato de licencia no describe para qué sirve el software licenciado, y cuáles son sus características principales, resultará muy difícil evaluar el alcance de las obligaciones del licenciante. Es que en este contexto, si el licenciario considerase que el software no cumple con la función para la cual lo adquirió y reclamase por ello, la única forma de resolver la disputa será apelando a las comunicaciones previas entre las partes, a otra documentación (por ejemplo, publicidad sobre el software), o bien a los usos y costumbres, que indicarán lo que razonablemente podría esperarse de un software como el estuviera en discusión. Afirma Veltani que resulta claro que no es conveniente dejar librado a alguna de estas alternativas la interpretación de algo tan relevante *como el alcance de las obligaciones del licenciante* y señala que el principio de interpretación *in dubio pro auctore* no servirá para llenar el vacío de la falta de regulación, por lo que sería un error para el licenciante pensar que al no describir el software licenciado está mejorando su posición en caso de conflicto. Lo recomendable es que la licencia describa cuál es la funcionalidad del software y cuáles son sus limitaciones, con expresa indicación de si se encuentra preparado para un uso profesional o si -por el contrario- sólo está habilitado el uso hogareño.

[1624]

Idem, p. 122. Precisa Veltani que si bien la autorización podría limitarse al uso

del software, también podría comprender su modificación, o incluso la creación de software o de otras obras. Esto es lo que ocurre, por ejemplo, cuando el software licenciado permite al usuario generar su propio código, sea para utilizar únicamente con ese software (v.g. los *scripts*), o bien para interactuar con otro software (como podría ocurrir con los lenguajes de programación). En cualquier caso, es conveniente que la licencia lo aclare en forma expresa: tanto el alcance de la autorización como cualquier *reivindicación* de derechos de propiedad intelectual que pudiera pretender el licenciante respecto de obras *creadas* con o *derivadas* del software licenciado. Pero el alcance de la licencia también debe aclarar (i) cómo se computará la cantidad de licencias, si el cómputo fuera diferente al tradicional de “una licencia por dispositivo”; y (ii) si la licencia es transferible de un dispositivo a otro.

[1625]

Idem, p. 123. Precisa Veltani que resulta conveniente incorporar una cláusula en el contrato de licencia en la que se deje constancia expresa de ciertas limitaciones específicas para el licenciatarario.

Podría pensarse que por aplicación del principio *in dubio pro auctore* esto no sería necesario, ya que todo aquello que no esté expresamente permitido por el autor, debería considerarse prohibido. Sin embargo, en el caso del software, a veces esta regla no puede aplicarse sin más y podrían surgir inconvenientes interpretativos si no se detallan ciertas limitaciones. Además, el hecho de que se incluyan de modo expreso en el contrato aventa toda posibilidad de que el licenciatarario pueda alegar desconocimiento o una interpretación alternativa.

[1626]

Idem, p. 124. Postula Veltani que resulta siempre conveniente dejar aclarado en la licencia, sobre todo cuando se trata de una licencia de software que fue desarrollado “a medida” o que fue adecuado a las necesidades del licenciatarario, si existe exclusividad o no. La licencia puede ser exclusiva o no, y la exclusividad -en su caso- puede darse con relación al ámbito territorial o a una determinada actividad.

Para evitar problemas de interpretación, lo aconsejable es que esto sea aclarado en el contrato de licencia, de un modo expreso. Si existe algún tipo de exclusividad, es aconsejable que se exprese en una cláusula que debería dejar constancia: (i) del tipo de exclusividad de que se trate (v.g. si es una exclusividad en un territorio determinado, etc.); y (ii) de las condiciones de vigencia de la exclusividad (porque podría ocurrir que la vigencia sea temporal o esté sujeta a alguna condición).

[1627]

Ibid.

[1628]

In re CNCom, Sala D, “Optimum S.A. c. Edenor S.A. Empresa Distribuidora Norte S.A. y otro”, JA 1999-III-326.^[1]_[SEP]

[1629]

Confr. Darío Veltani, *El contrato de licencia de software*, publicado en en Revista Derecho y Nuevas Tecnologías, N° 1, CeTyS, 2017, p. 125, nota 38.

[1630] Idem, p. 126, nota 39.

[1631] Ibid.

[1632] Idem, p. 127. Afirma Veltani que la finalidad de esta cláusula es que si el software licenciado falla y genera un daño -al licenciataro o a terceros que pudieran reclamar dichos daños al licenciataro- el monto a pagar por el licenciante no resulte inconmensurable. Teniendo presente que en muchas oportunidades resulta difícil establecer por qué falló el software (y en muchas el origen es la interacción con otros programas, la infraestructura de comunicaciones, o incluso el mal funcionamiento del hardware) y que las fallas pueden generar daños cuantiosos, *es fundamental que la cláusula limitativa de la responsabilidad esté presente en todo contrato de licencia de software*. Es una cláusula aceptada por nuestros tribunales en la medida en que no resulte de aplicación el estatuto de defensa del consumidor. Ahora bien, dado que el CCyC estableció ciertas restricciones para los contratos con cláusulas predispuestas que podrían resultar de aplicación a la cláusula limitativa de la responsabilidad del licenciante, la redacción de esta cláusula debe realizarse con mucho cuidado, procurando que no resulte abusiva. Señala Veltani que para limitar la responsabilidad del licenciante existen, básicamente, dos aspectos a considerar, que pueden combinarse: (i) la exclusión de ciertos rubros indemnizatorios; y (ii) la fijación de un límite máximo, considerado en dinero, por el que el licenciante deberá responder. Con relación al primero de ellos, es decir, la exclusión de *rubros indemnizatorios*, es habitual excluir la pérdida de información, el lucro cesante, la pérdida de chance, los daños físicos y el daño moral, entre otros. La razonabilidad de tales exclusiones estará vinculada directamente con la naturaleza del software licenciado. Así, por ejemplo, en la mayoría de los casos será razonable excluir como rubro la pérdida de información, pero ello no sería razonable si la finalidad del software licenciado fuese realizar copias de resguardo (backups). Por lo tanto, con toda razón afirma Veltani que la selección de los rubros a excluir debe guardar relación con la finalidad del software licenciado, que -además- debe ser explicitada en la licencia para que la cláusula limitativa de la responsabilidad resulte consistente. Respecto del segundo aspecto, es decir, la fijación de un límite para la responsabilidad, es necesario que el tope fijado también guarde razonable relación con la finalidad del software. Resulta evidente que cuando el software está destinado a un uso profesional, el límite debería ser superior al del software destinado a uso hogareño. Debe tenerse presente que cuando la cláusula limitativa de la responsabilidad ha sido redactada adecuadamente, este límite resultará de aplicación luego de excluir los rubros indemnizatorios identificados en la propia cláusula. Es habitual que se establezca como límite para la responsabilidad del licenciante el precio pagado por la licencia. Esto podría ser razonable, pero en la mayoría de las veces será insuficiente. Y el riesgo de que el límite sea insuficiente es que podría ser considerado como abusivo y, por lo tanto, declarado nulo por un

tribunal de justicia. En suma, para establecer un límite razonable a la responsabilidad del licenciante debe considerarse: (a) la finalidad del software (lo que permitirá entender los daños que podría ocasionar su falla); (b) los rubros indemnizatorios excluidos (lo que permitirá definir cuáles serán los rubros que compondrán la base indemnizatoria); y (c) el precio pagado por la licencia (que deberá compararse con los rubros que potencialmente deberían ser indemnizados para verificar si existe una relación razonable que permita establecer el precio como límite). En base a estas consideraciones, podrá definirse un límite que resulte razonable en caso de que el software falle y cause un daño.

[1633]

Idem, p. 130. Señala Veltani que en la licencia de software deberían preverse ciertas garantías mínimas que debe brindar el licenciante: (a) la no turbación por parte de terceros que funden sus reclamos en algún derecho de propiedad intelectual respecto del software; y (b) el funcionamiento del software de acuerdo con los parámetros técnicos descritos en el contrato de licencia. Con relación a la primera de las garantías mencionadas, es condición esencial del contrato de licencia de software que el licenciante sea titular o tenga derechos suficientes como para licenciar el software. Y, por lo tanto, debe responder por cualquier reclamo que pudiera formular un tercero con relación a la legitimidad y/o extensión de la licencia de software. Más aún, *es recomendable que a esta garantía no resulte de aplicación la limitación de la responsabilidad del licenciante porque ello equivaldría a consagrar un supuesto de mala fe contractual*. Respecto de la segunda garantía, resulta conveniente detallar las condiciones técnicas en las cuales el software debería funcionar adecuadamente. Quizás estas condiciones sean “de laboratorio”, porque podrían exigir que no exista interacción con otro software -salvo el software de base-, entre otras cosas. Pero la lógica de la cláusula es precisar en qué condiciones operativas el licenciante garantiza la funcionalidad del software. Si nada se dice y existe una diferencia entre las partes, estas condiciones mínimas deberán ser interpretadas por el juez que, en definitiva, deba resolver el conflicto. A estas garantías se suman las implícitas vinculadas con la responsabilidad por vicios ocultos, que deberán aplicarse al contrato de licencia atendiendo a sus particularidades.

[1634]

Idem, p. 131. Señala Veltani que respecto del primer aspecto, es aconsejable *mencionar expresamente la posibilidad de fallas* en virtud de errores en el hardware, deficiencias en la conexión a Internet, o incompatibilidades derivadas de la interacción con otro software (por ejemplo, de tipo firewall o antivirus). Si se diera alguno de estos casos, aun cuando desde el punto de vista objetivo el software no hubiera estado disponible para su correcta utilización por el usuario -lo que tornaría de aplicación la cláusula-, la falta de disponibilidad no resultaría relevante.

La segunda cuestión está vinculada con el modo en que se computará el tiempo durante el cual el software no funcionó: habitualmente en este tipo de cláusulas el

funcionamiento se garantiza tomando en consideración un porcentaje de tiempo, de modo tal que -por ejemplo-, el licenciante podría garantizar que el software funcionará ininterrumpidamente durante el 99,9% del tiempo. El cómputo del *tiempo* podría hacerse, por ejemplo, por “día”, por “mes”, o incluso por “año”. Afirma Veltani sobre el particular que es fácil advertir que según sea el tiempo que consideremos como “tiempo total” (día, mes o año, por ejemplo), el tiempo durante el cual el software podría no funcionar será distinto y definir si el cómputo es diario, mensual, anual, etc., no es suficiente: es necesario aclarar si dicho período (día, mes, año, etc.) debe considerarse como lo marca el calendario, o en forma móvil. En el primer caso, el cómputo se reiniciará indefectiblemente cada día, mes o año, lo que implicará que si el tiempo de indisponibilidad del software se acumula en el final de un período y el principio del siguiente, no implicará incumplimiento (por ejemplo, en el caso del cómputo anual, el software podría no funcionar durante las últimas 8 horas del 31 de diciembre de un año, y durante las primeras 8 horas del 1 de enero del año siguiente, sumando así 16 horas de indisponibilidad). En el segundo caso, en cambio, la medición deberá realizarse tomando como momento de inicio del cómputo el momento en que se verifique la indisponibilidad. Es decir, si estuviéramos bajo el esquema de medición anual, entonces lo que se garantizará es que en el término de un año, computados desde la fecha en que ocurrió la indisponibilidad, no se supere el límite comprometido. En el caso del ejemplo, si el 31 de diciembre el software no hubiera funcionado durante 8 horas, entonces hasta el 31 de diciembre del año siguiente no podría volver a fallar (si lo hiciera, estaría violado el nivel comprometido).

El tercer aspecto que una cláusula de *Service Level* debe regular es quién y cómo realizará la medición de la disponibilidad del software. Habitualmente, esta obligación quedará en cabeza del licenciante, dado que es razonable que así sea porque tiene más posibilidades técnicas de documentar el funcionamiento del software de un modo preciso.

Finalmente, el último punto que debe prever la cláusula es el referido a las consecuencias del incumplimiento -por parte del licenciante- del nivel de disponibilidad ininterrumpida del software. En este punto, lo habitual es que la consecuencia sea una penalidad preestablecida, y que generalmente estará vinculada con el precio pagado por la licencia. Ahora bien, para poder redactar -o negociar- adecuadamente esta cláusula, es necesario comprender en favor de quién se establece. Téngase presente que se trata de un compromiso que asume el licenciante y de una garantía que otorga al licenciatario, y ello podría llevar a pensar que la cláusula se establece en favor del licenciatario. *Pero ello no es así.* En realidad, la cláusula de niveles de servicio se incorpora en el contrato *en beneficio del licenciante*. Si esta cláusula no existiera, frente a un supuesto de falta de funcionamiento del software resultarían de aplicación los principios generales, según los cuales ello implicaría un incumplimiento del contrato por parte del licenciatario. Con la cláusula de niveles de

servicio, en la medida en que la falta de funcionamiento se verifique durante el tiempo establecido en la propia cláusula, *la única consecuencia será el pago de la penalidad*. El licenciatarario no podría reclamar otra compensación ni pretender que existió un incumplimiento contractual. La solución está en el mismo contrato, y es la compensación prevista en la cláusula respectiva (si existe tal previsión). Entonces, para que resulte válida, es fundamental que se permita al licenciatarario accionar judicialmente cuando se está por debajo del tiempo garantizado. Es decir, para que resulte válida, la cláusula debería establecer un esquema de responsabilidad para el licenciante que funcionaría de este modo: (a) si el software no estuviera disponible entre el 100% del tiempo y el 99,9% del tiempo, no existirá ninguna consecuencia para el licenciante; (b) si el software no estuviera disponible entre el 99,9% del tiempo y un porcentaje a definir (por ejemplo, el 95%), entonces la única compensación para el licenciatarario será la penalidad prevista en la cláusula; y (c) si el software no estuviera disponible por debajo de esa segunda línea (en el ejemplo, el 95%) entonces el licenciatarario podrá resolver el contrato y/o reclamar los daños y perjuicios que hubiera sufrido.

[1635]

Los términos y condiciones revisados están disponibles al 10/05/2020 en <https://hodly.com/static/pdf/terms.pdf>

[1636]

Confr. Michael Rustad y Marta Vittoria Onufrio, en *The Exportability of the Principles of Software: Lost in Translation?* Recuperado el 10/05/2020 en <http://scienceandtechlaw.org/wp-content/uploads/2015/10/The-Exportability-of-the-Principles-of-Software-Lost-in-Translation.pdf>, p. 26.

[1637]

Disponible, al 10/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0024&from=EN>.

[1638]

Disponible, al 10/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0083&from=en>

[1639]

Idem, véase Art. 16, inc. m), y lo sostenido por Michael Rustad y Marta Vittoria Onufrio, en *The Exportability of the...o.c.*, p. 59 –en relación al texto de la derogada Directiva sobre Ventas a Distancia y Consumidores, que fue reemplazada en el año 2011 por la nueva Directiva de Protección de Consumidores, manteniendo tal excepción al derecho al desistimiento. Mismo criterio sigue nuestro CCCN, véase Art. 1116, inc. b), que reza: “*Excepciones al derecho de revocar. Excepto pacto en contrario, el derecho de revocar no es aplicable a los siguientes contratos: (b) los de suministro de grabaciones sonoras o de video, de discos y de programas informáticos que han sido decodificados por el consumidor, así como de ficheros informáticos, suministrados por vía electrónica, susceptibles de ser descargados o reproducidos con carácter inmediato para su uso permanente.*” El resaltado es mío. ^[1]_[SEP]

[1640] Disponible, al 10/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32005L0029&from=EN>

[1641] Disponible, al 10/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0031&from=EN>

[1642] Idem, Art. 9.

[1643] Disponible, al 10/05/2020 en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:01993L0013-20111212&from=EN>

[1644] Idem, Art. 5.

[1645] Confr. Michael Rustad y Marta Vittoria Onufrio, en *The Exportability of the Principles of Software: Lost in Translation?..o.c.*, p. 67.

[1646] Idem, p. 77.

[1647] Ibid.

[1648] Confr. <https://asiatimes.com/2019/05/binance-offers-full-refund-after-40m-hack/> disponible al 10/05/2020. En Mayo de 2019, el *Exchange* más grande del mundo fue hackeado a través de una falla de seguridad en su *hot Wallet* y se robaron criptoactivos por valor de 40 millones de Dólares de sus usuarios. El *Exchange* ofreció reembolso total a sus usuarios.

[1649] Confr. <https://www.bloomberg.com/news/articles/2018-01-27/coincheck-to-repay-customers-who-lost-money-in-400-million-hack>, recuperado el 10/05/2020. Véase también <https://www.wsj.com/articles/hacked-japanese-cryptocurrency-exchange-pays-back-customers-1520917328>, recuperado en la misma fecha.

[1650] Confr. <https://www.computerworld.com/article/3389678/whats-a-crypto-wallet-and-does-it-manage-digital-currency.html>, recuperado el 10/05/2020.

[1651] Véase por ejemplo <https://paper.dash.org>

[1652] Véase por ejemplo <https://www.exodus.io> y <https://www.dash.org/downloads/>

[1653] Otro ejemplo de cold hardware Wallet es https://shop.trezor.io/?offer_id=10&aff_id=1035

[1654] Confr. <https://www.computerworld.com/article/3389678/whats-a-crypto-wallet-and-does-it-manage-digital-currency.html>, recuperado el 10/05/2020

[1655] Confr. <https://blogs.gartner.com/avivah-litan/2019/09/26/can-mpc-rescue-us-blockchain-private-keys/>, recuperado el 10/05/2020.

[1656] Confr. <https://blogs.gartner.com/avivah-litan/2019/09/26/can-mpc-rescue-us-blockchain-private-keys/>, recuperado el 10/05/2020.

[1657] Confr. <https://tokenpost.com/Bakkt-reveals-125M-insurance-coverage-for-bitcoin-stored-in-Bakkt-Warehouse-3362>, recuperado el 10/05/2020. Ampliar sobre esta interesante plataforma de futuros sobre criptoactivos en <https://medium.com/the-green-light/what-is-bakkt-complete-exchange-guide-ab60b45c5c47>, recuperado el 10/05/2020.

[1658] Confr. <https://blogs.gartner.com/avivah-litan/2019/09/26/can-mpc-rescue-us-blockchain-private-keys/>, recuperado el 10/05/2020.

[1659] Confr. *Report from Study Group on Virtual...o.c.*, p. 3.

[1660] Confr. Michel Rauchs, Apolline Blandin, Kristina Klein, Gina Pieters, Martino Recanatini, y Bryan Zhang, *2nd Global Cryptoasset Benchmarkings...o.c.* p. 53.

[1661] Confr. <https://economictimes.indiatimes.com/wealth/personal-finance-news/rbi-issues-consumer-protection-rules-for-mobile-wallets-users-liability-limited/articleshow/67416793.cms>, disponible al 10/05/2020.

[1662] Véase, Ley N° 25.065, Capítulo X.

[1663] Ampliar en <https://www.mondaq.com/india/fin-tech/904716/bitcoin-back-in-business-supreme-court-strikes-down-rbi-circular-prohibiting-banking-services-to-cryptocurrency-businesses>, disponible al 13/05/2020.

[1664] Ibid. Se afirma en la nota citada que: *“For now, there remains some uncertainty about the future of the Cryptocurrency industry in India, also in the context of the Banning of Cryptocurrency & Regulating of Official Digital Currency Bill, 2019 (Bill), which proposes the ban of private Cryptocurrencies and the criminalisation of their use. The Bill has not yet been brought to the Indian Parliament for a vote, however, and is thus subject to revision. Further, **the Bill proposes the creation of a 'digital rupee' that the central government and the RBI would have a monopoly over, so the government's general position on Cryptocurrencies is clearly not as unfavourable as it once was.** Whether this will extend to an acceptance of decentralised, non-government Cryptocurrencies – and whether private players will be permitted to participate in an Indian Cryptocurrency market that has significant scope for growth – remains to be seen, and we expect to see significant developments in this space in the coming months.”*El resaltado es mío.

[1665] Confr. Michel Rauchs, Apolline Blandin, Kristina Klein, Gina Pieters, Martino Recanatini, y Bryan Zhang, *2nd Global Cryptoasset Benchmarkings...*o.c. p. 56.

[1666] Ibid.

[1667] Confr. Gabrielle Patrick y Anurag Bana, miembros del IBA Legal Policy & Research Unit Legal Paper, en *Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World*, recuperado el 10/05/2020 en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwi5zPvGwqnpAhUDHrkG520D-45FA-A29B-EF019A7D7FC9&usg=AOvVaw1Wtx9ZZkf0ltdfa1eqvS_f, p. 43.

[1668] Véase <https://www.parity.io>

[1669] Para ampliar sobre cuáles fueron los *bugs* detectados y explotados, véase: https://www.vice.com/en_us/article/ywbqmg/parity-multi-signature-wallet-vulnerability-300-million-hard-fork,

[1670] Confr. <https://www.parity.io/the-multi-sig-hack-a-postmortem/> disponible al 10/05/2020.

[1671] Confr. <https://www.parity.io/announcing-the-bug-bounty-program/>, disponible al 10/05/2020.

[1672] Confr. <https://www.parity.io/bug-bounty/#reward> disponible al 10/05/2020.

[1673] Confr. <https://www.parity.io/security-alert-2/>, disponible al 10/05/2020. Puede ampliarse en https://www.vice.com/en_us/article/ywbqmg/parity-multi-signature-wallet-vulnerability-300-million-hard-fork, disponible al 10/05/2020.

[1674] Confr. <https://es.cointelegraph.com/news/eip-999-why-a-vote-to-release-parity-locked-funds-evoked-so-much-controversy> disponible al 10/05/2020.

[1675] Confr. <https://www.criptonoticias.com/seguridad-bitcoin/vulnerabilidades/40-nodos-parity-ethereum-vulnerables-ataque-dos/> y ampliar en https://srlabs.de/bites/blockchain_patch_gap/ disponible al 10/05/2020.

[1676] Confr. <https://www.parity.io/new-parity-ethereum-update-fixes-several-rpc-vulnerabilities/> disponible al 10/05/2020.

[1677] Confr. <https://news.crypterium.com/10-ways-to-hack-a-bitcoin-wallet-in-2020/>, recuperado al 10/05/2020.

[1678] Véase <https://www.kaspersky.es/blog/cryptoshuffler-bitcoin-stealer/14701/>, disponible al 10/05/2020. Se trata de un troyano, conocido como *CryptoShuffler*, que

reside en la memoria de la computadora, y monitoriza el portapapeles y el almacenamiento temporal destinado a las operaciones de cortar y pegar. Cuando CryptoShuffler detecta la dirección de una wallet en el portapapeles (es muy fácil hacerlo por la longitud de la línea y los caracteres específicos), la reemplaza por otra. Como resultado, la transferencia de criptomonedas se realiza, solo que el destinatario son los hackers responsables de CryptoShuffler.

[1679] Confr. *Report from Study Group on Virtual...o.c.*, p. 6.

[1680] Confr. Andrés Chomczyk, *Reflexiones respecto de la regulación de la industria fintech a partir del dictado de las comunicaciones "A" 6859 y "A" 6885 sobre los proveedores de servicios de pago*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.

[1681] Ibid.

[1682] En la Unión Europea el dinero electrónico está regulado en la Directiva 2009/110/CE, que lo define como "*todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago [...] y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico*". Ampliar en Santiago Mora, *Una actualización sobre el dinero electrónico*, Revista Derecho y Nuevas Tecnologías (RDYNT), CETYS-UDESA, 2017-1.

[1683] Confr. Juan Diehl Moreno, Diego Fernández y Santiago Eraso Lomaquíz, *Consideraciones sobre la nueva normativa aplicable a los prestadores de servicios de pago*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley. Afirman los autores citados que los fondos son transferidos por el usuario al emisor con anterioridad a la emisión del medio de pago, y clasifican el dinero electrónico según los siguientes criterios: (i) el tipo de entidad emisora; (ii) su aptitud para circular, (iii) el tipo de soporte en el que se encuentren almacenados; y (iv) la posibilidad de recarga de aquel soporte. En cuanto al tipo de entidad emisora, se ha llamado dinero electrónico bancario a aquel emitido por entidades financieras y no bancario, a aquel emitido por empresas que no poseen tal carácter. Señalan que algunas legislaciones han desarrollado un tipo de autorización especial para las emisoras de dinero electrónico, las cuales cuentan con un régimen similar al de las entidades financieras, pero atenuado en atención a sus características especiales y objeto limitado.

[1684] Ibid. Señalan los autores que el dinero de curso legal es una cosa fungible, siendo de aplicación el Art. 1367, CCCN. Sin embargo, la mera recepción de fondos para la emisión de un medio de pago electrónico no permitiría, prima facie, incluir a las emisoras de dinero electrónico en la categoría de las entidades financieras en tanto

no hagan intermediación financiera en los términos de la Ley de Entidades Financieras N° 21.526.

[1685]

Ibid. El autor citado recuerda lo dispuesto por los Arts. 4, inc. g) y Art. 47, inc. f) de la Ley N° 24.144: “Art. 4° — *Son funciones y facultades del banco:*

a) *Regular el funcionamiento del sistema financiero y aplicar la Ley de Entidades Financieras y las normas que, en su consecuencia, se dicten;*

b) *Regular la cantidad de dinero y las tasas de interés y regular y orientar el crédito;*

c) *Actuar como agente financiero del Estado nacional y depositario y agente del país ante las instituciones monetarias, bancarias y financieras internacionales a las cuales la Nación haya adherido, así como desempeñar un papel activo en la integración y cooperación internacional;*

d) *Concentrar y administrar sus reservas de oro, divisas y otros activos externos;*

e) *Contribuir al buen funcionamiento del mercado de capitales;*

f) *Ejecutar la política cambiaria en un todo de acuerdo con la legislación que sancione el Honorable Congreso de la Nación;*

g) ***Regular, en la medida de sus facultades, los sistemas de pago, las cámaras liquidadoras y compensadoras, las remesadoras de fondos y las empresas transportadoras de caudales, así como toda otra actividad que guarde relación con la actividad financiera y cambiaria;***

h) *Proveer a la protección de los derechos de los usuarios de servicios financieros y a la defensa de la competencia, coordinando su actuación con las autoridades públicas competentes en estas cuestiones.*

En el ejercicio de sus funciones y facultades, el banco no estará sujeto a órdenes, indicaciones o instrucciones del Poder Ejecutivo nacional, ni podrá asumir obligaciones de cualquier naturaleza que impliquen condicionarlas, restringirlas o delegarlas sin autorización expresa del Honorable Congreso de la Nación.” El resaltado es mío.

“Art. 47. *Son facultades del superintendente:*

a) *Vigilar el cumplimiento del régimen informativo y contable para las entidades financieras y cambiarias;*

b) *Disponer la publicación de los balances mensuales de las entidades financieras, estados de deudores y demás informaciones que sirvan para el análisis de la situación del sistema;*

c) *Ordenar a las entidades que cesen o desistan de llevar a cabo políticas de préstamos o de asistencia financiera que pongan en peligro la solvencia de las mismas;*

d) *Aplicar las sanciones que establece la Ley de Entidades Financieras por infracciones cometidas por las personas o entidades, o ambas a la vez, a sus disposiciones, las que, sin perjuicio de la facultad de avocación del presidente, sólo serán impugnables por las vías contempladas en su artículo 42;*

e) *Ejercer las demás facultades que las leyes otorgan al banco relativas a la superintendencia, con excepción de las expresamente atribuidas por esta ley al directorio*

del banco;

f) **Aplicar las disposiciones legales que sobre el funcionamiento de las denominadas tarjetas de crédito, tarjetas de compra, dinero electrónico u otras similares, dicte el Honorable Congreso de la Nación y las reglamentaciones que en uso de sus facultades dicte el Banco Central de la República Argentina.**” El resaltado es mío.

[1686]

Confr. Andrés Chomczyk, *Reflexiones respecto de la regulación de la industria fintech...*o.c.

[1687]

Se sigue, en general y con las adaptaciones del caso, el artículo del autor titulado *Banca vs. Fintech: Round 1*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.

[1688]

Confr. Comunicación “A” 6154 del 13/01/2017, disponible al 8/05/2020 en <http://www.bcra.gov.ar/pdfs/comytexord/A6154.pdf> y Comunicación “A” 6885 del 30/01/2020, disponible al 08/02/2020 en <http://www.bcra.gov.ar/Pdfs/comytexord/A6885.pdf>.

Andrés Chomczyk, en *Reflexiones respecto de la regulación de la industria fintech a partir del dictado de las comunicaciones..*o.c. señala que las funciones que tienen asignados los PSPs guardan más relación con la actividad de emisión y gestión de dinero electrónico, a pesar de que la regulación sobre PSPs los defina como “las personas jurídicas que, sin ser entidades financieras, **cumplan al menos una función dentro de un esquema de pago minorista, en el marco global del sistema de pagos**”. Afirma el autor citado que el nombre elegido para estas entidades –PSPs– no es apropiado para las funciones que tienen asignadas. También se señala que tres normas dictadas por la AFIP i.e. Resoluciones Generales 4614/2019, 4647/2019 y 4622/2019 usan una definición propia para estas entidades, como entidades que “administren servicios de procesamiento de pagos a través de plataformas de gestión electrónica o digital, residentes o domiciliados en el país”, a las que define como *proveedores de procesamiento de pagos a través de plataformas de gestión electrónica o digital*. AFIP también se refiere a entidades que “administran, gestionan, controlan o procesan movimientos de activos a través de plataformas de gestión electrónicas o digitales, por cuenta y orden de personas humanas y jurídicas residentes en el país o en el exterior”, a las que define como *proveedores de servicios de administración e intermediación de cuentas virtuales, billeteras virtuales, inversión y financiamiento*, donde también se incluye a los “sujetos que administren servicios electrónicos de pagos y/o cobranzas por cuenta y orden de terceros, **incluso a través del uso de dispositivos móviles y/o cualquier otro soporte electrónico, comprendidos los virtuales**”. Afirma el autor citado que si bien cada entidad tiene competencia para regular dentro de su área, es cierto que el BCRA, como regulador del sector financiero, tiene la posibilidad de facilitar la tarea de organizar el sector y brindar armonía en cuanto a las categorías. Los resaltados son míos.

[1689] Confr. Alejandro E. Kulik,^[1] *Comunicaciones “A” 6859 y “A” 6885 BCRA*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.

[1690] Confr. Comunicación “A” 6885, apartado 1.1.2.

[1691] Art. 10, Ley N° 21.526 de Entidades Financieras: *“No podrán desempeñarse como promotores, fundadores, directores, administradores, miembros de los consejos de vigilancia, síndicos, liquidadores o gerentes de las entidades comprendidas en esta Ley:*
a) *Los afectados por las inhabilidades e incompatibilidades establecidas por el artículo 264 de la Ley número 19.550;*
b) *Los inhabilitados para ejercer cargos públicos;*
d) *Los inhabilitados para ser titulares de cuentas corrientes u otras que participen de su naturaleza, hasta tres años después de haber cesado dicha medida;*
e) *Los inhabilitados por aplicación del inciso 5) del artículo 41 de esta ley, mientras dure el tiempo de su sanción, y*
f) *Quienes por decisión de autoridad competente hubieran sido declarados responsables de irregularidades en el gobierno y administración de las entidades financieras.*
Sin perjuicio de las inhabilidades enunciadas precedentemente, tampoco podrán ser síndicos de las entidades financieras quienes se encuentren alcanzados por las incompatibilidades determinadas por el artículo 286, incs. 2 y 3, de la Ley 19.550.”

[1692] Confr. Comunicación “A” 6885, apartado 1.1.5.

[1693] Confr. Comunicación SINAP “A” 6510, del 15/05/2018, disponible al 9/01/2020 en <http://www.bcra.gov.ar/Pdfs/comytexord/A6510.pdf>. Otras normas que indirectamente se refieren a los PSPs (o a su gama de servicios) son la Comunicación “A” 5982 sobre Plataformas de Pagos Móviles (luego reemplazada por la Comunicación “A” 6669 y modifs.); la Comunicación “A” 6154 que regula los Servicios Complementarios de la Actividad Financiera (luego reemplazada por la Comunicación “A” 6277 y modifs.), y la Comunicación “A” 6668 y modif. que regula el uso del Código QR.

[1694] Confr. <https://www.cronista.com/finanzasmercados/Llega-la-CVU-clave-para-operar-con-billeteras-digitales-en-el-mundo-fisico-20180517-0055.html> disponible al 08/05/2020.

[1695] Confr. <https://www.cronista.com/finanzasmercados/Mercado-Pago-sumo-un-millon-de-cuentas-comitentes-y-ya-representa-el-75-del-total-de-los-Fondos-20191126-0021.html> disponible al 8/05/2020.

[1696] Confr. <https://www.infotechnology.com/negocios/Con-record-de-cuentas-en-la-Argentina-MercadoPago-apunta-a-Mexico-20191128-0009.html> recuperado al

8/05/2020.

[1697]

Confr. https://www.mercadopago.com.ar/ayuda/términos-y-condiciones-de-inversiones_4070 versión 10/10/2019, recuperado el 31/01/2020. Estos términos fueron modificados conforme a la nueva regulación del BCRA citada en la nota siguiente.

[1698]

Disponible en <http://www.bcra.gov.ar/Pdfs/comytexord/A6859.pdf> recuperado el 8/05/2020.

[1699]

Con gran tino, Andrés Chomczyk, *Reflexiones respecto de la regulación de la industria fintech...*o.c. señala que la norma no aclara si el usuario podrá (o no) elegir el fondo común de dinero al cual transferir sus fondos, o si se encuentra limitado en cuanto a la oferta que haga el PSP. La cuestión no es menor, puesto que la situación podría ser pasible de ser calificada como “venta atada”, la cual se encuentra ahora prohibida por el Código Civil y Comercial de la Nación en su Art. 1099, pero era una práctica anticompetitiva ya prohibida desde mucho tiempo antes, por la vieja ley antitrust N° 25.156 del año 1999, y también está expresamente prohibida en la nueva Ley de Defensa de la Competencia N° 27.442, en su Art. 3, inc. f) y g). Asimismo, señala el autor citado que es preocupante que el BCRA no haya reparado en la información que los PSP deben a sus clientes en cuanto a la oferta de estos productos financieros. Se acuerda con Chomczyk que estos temas deben ser tratados en el futuro con una solución idónea para el cliente y poniendo el foco en lograr mayor apertura y competencia entre los actores del sector.

[1700]

Confr. Alejandro E. Kulik,^[17]_[SEP] *Comunicaciones “A” 6859 y “A” 6885 BCRA...*o.c. puntualiza que

respecto de la posibilidad de invertir los fondos de los usuarios por parte de los PSP, se encuentran dos posiciones diferentes: (i) aquellos países que no limitan en absoluto esta posibilidad, y (ii) los que la restringen de manera parcial, permitiendo la inversión siempre que sea en instrumentos líquidos y seguros, de modo de poder satisfacer las demandas de retiro de fondos de los clientes. Afirma el autor citado que dentro de esta última posición existen matices entre las jurisdicciones que permiten cualquier clase de inversión que reúna las características de seguridad y liquidez, y aquellas que limitan las posibilidades de inversión al exigir que los fondos se encuentren depositados en cuentas de entidades financieras sujetas a regulación prudencial (ya sea una sola entidad o varias). Así, países como India, Estados Unidos, Perú, Brasil y Uruguay prefieren una mayor diversificación de las inversiones, por lo que requieren la inversión de una parte de los fondos en activos líquidos y seguros, como por ejemplo títulos de deuda pública. Por su parte, la Unión Europea permite a los PSP que no posean el 100% de los fondos de los usuarios depositados en cuentas bancarias, siempre y cuando contraten un seguro que garantice la porción de los fondos no

depositada. Sobre el particular, el BCRA ha decidido adoptar una restricción a las posibilidades de inversión de los fondos de los usuarios por parte de los PSP, al exigir que el 100% de los fondos de los clientes se encuentre depositado —en todo momento— en cuentas a la vista en pesos en entidades financieras del país. Afirma Kulik que dado que no se lo ha regulado expresamente, este requisito se puede cumplir a través del depósito en una única entidad financiera o mediante la diversificación de los depósitos en más de una entidad. Esta última opción, si bien podría implicar una disminución en los rendimientos de los fondos depositados para el PSP, minimiza aún más el riesgo de insolvencia (en este caso, el relativo a los bancos) al distribuir los fondos en más de una entidad.

[1701]

Confr. Comunicación “A” 6762, T.O. al 22/08/2019, recuperada el 8/05/2020 en <https://www.bcra.gob.ar/Pdfs/Textord/t-depaho.pdf>. Andrés Chomczyk, *Reflexiones respecto de la regulación de la industria fintech...o.c.* señala que los fondos de los clientes pueden estar depositados en una única cuenta o en una cuenta para cada usuario, mientras se trate de cuentas en el sistema financiero local y haya un sistema para saber la tenencia de cada usuario. Con independencia de la alternativa seleccionada, el PSP debe ser capaz de identificar qué fondos corresponden a cada usuario.

Afirma el autor citado que en lo atinente a los fondos operativos del PSP, deben estar separados en otra cuenta a la vista para mantener separados sus fondos del dinero de sus clientes, evitando así cualquier tipo de uso de aquellos. Se afirma que este elemento también resulta un aspecto esencial de los sistemas de dinero electrónico, y configura otro elemento que lleva a pensar que el BCRA ha ingresado en la creación de una regulación del dinero electrónico, facultad reservada al Congreso de la Nación, más que en una regulación del sistema de pagos minorista.

[1702]

Disponible al 09/05/2020 en <http://www.bcra.gov.ar/Pdfs/comytexord/A6885.pdf>

[1703]

La inscripción se tramita desde el portal de AFIP, y debe realizarse adjuntando: (i) copia del contrato social o estatuto y de todas sus modificaciones (en archivo con formato “.pdf”); (ii) datos del PSP: (a) denominación social, marca comercial, CUIT, domicilio legal, domicilio especial; (b) datos del representante legal o apoderado; (c) datos del responsable de la seguridad de los datos; (d) datos del responsable para vigilancia de sistemas de pago; (e) datos del responsable para régimen informativo; (iii) descripción operativa y comercial, incluyendo descripción de los servicios de pago que serán provistos y los medios de pago que involucra, cuentas de pago que ofrezca, incluyendo sus términos y condiciones específicas incluyendo la utilización de CVUs; esquemas de pago en los que cumpla función de administrador, incluyendo la declaración de todos sus participantes; esquemas de pago en los que participe en una función diferente a la de administrador, especificando las funciones que asuma en cada

caso y los modos de restitución de fondos en caso de ser ello requerido o cesar la actividad; (iv) identificación de los accionistas y directivos, identificando a las personas humanas que posean al menos el 20% del capital y/o votos de la persona jurídica o que por otros medios ejerzan el control final, directo o indirecto del PSP (principales integrantes del órgano de gobierno), e identificando a quienes integran el órgano de administración o fiscalización; y (v) una declaración jurada de que la totalidad de la información presentada por medios electrónicos es verdadera, que la documentación es copia fiel y que los originales están a disposición de la SEFyC, indicando el lugar donde se encuentran.

[1704] Confr. Comunicación “A” 6885, apartado 3.2.

[1705] Confr. Alejandro E. Kulik,^[1]_{SEP} *Comunicaciones “A” 6859 y “A” 6885 BCRA...o.c.*

[1706] Ibid. Señala Kulik que para cumplir con el objetivo de separar los fondos propios de los fondos de terceros, se advierte un consenso en la legislación internacional respecto de la necesidad de exigir a los PSPs aislar los fondos de sus usuarios de los activos propios. La forma en que tal separación se consigue depende del sistema jurídico imperante en cada país. Así, en Estados que aplican el common law, el requisito se resuelve aplicando el concepto jurídico del *trust*, figura jurídica a través de la cual una persona transmite bienes a otra que gestiona los bienes en favor de uno o más beneficiarios. En el ecosistema de los PSP, el rol de la persona que gestiona los bienes en favor de los beneficiarios podría ser desempeñado por el propio PSP o por cualquier persona física o jurídica que pase a ser responsable de la gestión de los fondos de los usuarios. En este modelo, hay una persona que gestiona los fondos, pero, legalmente, la propiedad de los fondos sigue siendo de los usuarios. Lo trascendente del esquema planteado radica en que los fondos administrados por el PSP dejan de considerarse como recursos propios del PSP. En consecuencia, los fondos de los usuarios no pueden ser utilizados para atender las obligaciones del proveedor en caso de quiebra. Señala Kulik que esta clase de regulaciones se encuentra en países como Kenia, Afganistán y Estados Unidos. Existen otras jurisdicciones en las cuales este sistema está disponible en su ordenamiento jurídico para ser utilizado, pero no se ha dispuesto un requisito específico para emplearlo en relación con los PSP, tal el caso de la India.

Por su parte, en aquellos Estados de tradición jurídica latina se utiliza la figura contractual del fideicomiso, que presenta sujetos y relaciones entre ellos similares a los del trust. Esta solución ha sido implementada en Paraguay, Perú y Uruguay. En los países en los que no existe ninguna de las figuras jurídicas mencionadas anteriormente, se han incluido disposiciones específicas en las regulaciones a los PSP para garantizar que los fondos estén aislados y segregados de los activos del proveedor. Ejemplo de ello lo configura la normativa europea, la cual establece que los fondos de dinero electrónico no deben mezclarse en ningún momento con cualquier otro activo,

y que estos fondos deben separarse en beneficio de los clientes frente a los reclamos de otros acreedores del PSP. Así, con relación al riesgo de liquidez entre las diversas opciones disponibles, el BCRA ha resuelto seguir los lineamientos de la normativa europea, exigiendo el depósito de fondos propios en una una cuenta a la vista 'operativa' (de libre disponibilidad) distinta a la cuenta donde se encuentren depositados los fondos de los clientes.

[1707]

Art. 41, Ley N° 21.526. — Quedarán sujetas a sanción por el Banco Central de la República Argentina las infracciones a la presente ley, sus normas reglamentarias y resoluciones que dicte el Banco Central de la República Argentina en ejercicio de sus facultades.

Las sanciones serán aplicadas por el presidente del Banco Central de la República Argentina, o la autoridad competente, a las personas o entidades o ambas a la vez, que sean responsables de las infracciones enunciadas precedentemente, previo sumario que se instruirá con audiencia de los imputados, con sujeción a las normas de procedimiento que establezca la indicada institución y podrá consistir, en forma aislada o acumulativa, en:

1. Llamado de atención.
2. Apercibimiento.
3. Multas.
4. Inhabilitación temporaria o permanente para el uso de la cuenta corriente bancaria.
5. Inhabilitación temporaria o permanente para desempeñarse como promotores, fundadores, directores, administradores, miembros de los consejos de vigilancia, síndicos, liquidadores, gerentes, auditores, socios o accionistas de las entidades comprendidas en la presente ley. (Inciso modificado por el Art. 3° de la Ley N° 24.485 B.O. 18/4/1995)
6. Revocación de la autorización para funcionar.

El Banco Central de la República Argentina reglamentará la aplicación de las multas, teniendo en cuenta para su fijación los siguientes factores:

- Magnitud de la infracción.
- Perjuicio ocasionado a terceros.
- Beneficio generado para el infractor.
- Volúmen operativo del infractor.
- Responsabilidad patrimonial de la entidad.

Si del sumario se desprendiere la comisión de delitos, el Banco Central de la República Argentina promoverá las acciones penales que correspondieran, en cuyo caso podrá asumir la calidad de parte querellante en forma promiscua con el ministerio fiscal.

[1708]

Art. 42, Ley 21.562. — Las sanciones establecidas en los incisos 1) y 2) del artículo anterior, sólo serán recurribles por revocatoria ante el presidente del Banco Central de la República Argentina.

Aquellas sanciones a las que se refieren los incisos 3), 4), 5) y 6) del artículo anterior, serán apelables, al solo efecto devolutivo por ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal de la Capital Federal.

En el caso del inciso 6, hasta tanto se resuelva el recurso, dicha Cámara dispondrá la intervención judicial de la entidad sustituyendo a los representantes legales en sus derechos y facultades.

Los recursos deberán interponerse y fundarse ante el Banco Central de la República Argentina dentro de los quince (15) días hábiles a contar desde la fecha de notificación de la resolución. Si el recurso fuera de apelación, las actuaciones deberán elevarse a la Cámara dentro de los quince (15) días hábiles siguientes.

Para el cobro de las multas aplicadas en virtud del inciso 3) del artículo anterior, el Banco Central de la República Argentina seguirá el procedimiento de ejecución fiscal previsto en el Código Procesal Civil y Comercial de la Nación. Constituirá título suficiente la copia simple de la resolución que aplicó la multa, suscrita por dos firmas autorizadas del Banco Central de la República Argentina, sin que puedan oponerse otras excepciones que la de prescripción, espera y pago documentados.

La prescripción de la acción que nace de las infracciones a que se refiere este artículo, se operará a los seis (6) años de la comisión del hecho que la configure. Ese plazo se interrumpe por la comisión de otra infracción y por los actos y diligencias de procedimientos inherentes a la sustanciación del sumario, una vez abierto por resolución del presidente del Banco Central de la República Argentina. La prescripción de la multa se operará a los tres (3) años contados a partir de la fecha de notificación de dicha sanción firme.

Los profesionales de las auditorías externas designadas por las Entidades Financieras para cumplir las funciones que la ley, las normas reglamentarias y las resoluciones del Banco Central de la República Argentina dispongan, quedarán sujetas a las previsiones y sanciones establecidas en el artículo 41 por las infracciones al régimen. Las Sociedades Calificadoras de Riesgo, sus integrantes profesionales intervinientes y cualquier otra persona física o jurídica que en el ejercicio de sus funciones o con motivo de una profesión o título habilitante, produjera informes u opiniones técnicas de cualquier especie, en infracción o contrarios a las normas de su arte, oficio o profesión, quedarán también sujetos por las consecuencias de sus actos a las previsiones y sanciones del artículo 41.

[1709]

Confr. <http://camarafintech.com.ar/wp-content/uploads/2019/06/Informe-Ecosistema-Fintech-Argentino.pdf> recuperado el 8/05/2020, p. 13.

[1710]

Ibid, p. 15.

[1711]

Ibid, p. 16.

[1712]

Confr. <https://www.afluenta.com/informacion-sobre-afluenta>

[1713] Ibid., p. 26.

[1714] Ibid., p. 37.

[1715] Confr. BCRA, informe de inclusión financiera 2019, recuperado el 8/05/2020 de <https://camarafintech.com.ar/wp-content/uploads/2020/01/Banco-Central-de-la-República-Argentina.pdf> p. 5.

[1716] Confr. <http://camarafintech.com.ar/wp-content/uploads/2019/06/Informe-Ecosistema-Fintech-Argentino.pdf> recuperado el 8/05/2020, p. 52.

[1717] Ibid.

[1718] Disponible al 8/05/2020 en http://www.mineco.gob.es/stfls/mineco/prensa/noticias/2014/180711_AP_Ley_transfo

[1719] Confr. <https://www.asociacionfintech.es/noticias-del-sector/la-aprobacion-del-sandbox-situa-a-espana-como-uno-de-los-paises-mas-avanzados-en-el-ambito-de-la-regulacion-fintech/> recuperado al 8/05/2020.

[1720] Confr. http://www.mineco.gob.es/stfls/mineco/prensa/ficheros/noticias/2018/190222_np_digi recuperado al 8/05/2020.

[1721] Confr. Proyecto de ley, Exposición de motivos, p. 2.

[1722] Confr. El Proyecto, en su Arts. 10 a 16, establece siete garantías, especialmente intensas en caso de que en las pruebas participen clientes: consentimiento informado y protección de datos; derecho de desistimiento en todo momento; responsabilidad del promotor en caso de daños y perjuicios patrimoniales que sean consecuencia directa de la realización de pruebas; una garantía por daños; confidencialidad; seguimiento del supervisor durante todo el ejercicio de pruebas; y, finalmente, posibilidad de interrupción de las pruebas, entre otros, en caso de mala práctica o incumplimiento de la legislación o del protocolo.

[1723] Confr. El Art. 18 del Proyecto dispone: “...los plazos del procedimiento **se reducirán a la mitad**. Asimismo, podrán exigir, únicamente, la acreditación de los requisitos de los que no hubieran tenido conocimiento durante las pruebas...” (el resaltado es mío).

[1724] Confr. El Art. 19 del Proyecto reza:

“1. Conforme a lo previsto en el artículo 4 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, cuando haya de exigirse el cumplimiento de requisitos para el desarrollo de una actividad financiera, **las autoridades deberán aplicar el principio de**

proporcionalidad y elegir la medida menos restrictiva, motivar su necesidad para la protección del interés público así como justificar su adecuación para lograr los fines que se persiguen, **sin que en ningún caso se produzcan diferencias de trato discriminatorias**.

2. En particular, las autoridades competentes para autorizar podrán ponderar la exigencia de requisitos dentro del margen de apreciación nacional existente con arreglo a la legislación europea aplicable en cada caso. En concreto, siempre dentro de dicho margen de apreciación, **podrán ponderar los requisitos exigibles a los integrantes del órgano de administración y los correspondientes a la idoneidad de los accionistas, la estructura interna y el capital inicial**. Tal ponderación será motivada y tendrá en cuenta las directrices establecidas para los procesos de autorización por las autoridades europeas con competencias de supervisión.

3. Las autoridades supervisoras tendrán en cuenta el desarrollo y resultado de las pruebas contempladas en esta ley a efectos de aplicar, en su caso, medidas de proporcionalidad en supuestos similares dentro del margen de apreciación de que dispongan en su actividad supervisora con arreglo a la legislación específica aplicable.

4. El desarrollo y resultado de las pruebas se tendrá igualmente en cuenta a los efectos del cumplimiento de lo dispuesto para los procedimientos de elaboración de normas legales y reglamentarias en el artículo 26 de la Ley 50/1997, de 27 de noviembre, del Gobierno. En particular, conforme a lo dispuesto en los artículos 129 y 130 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se valorará la incidencia de la aplicación de las nuevas tecnologías en el principio de proporcionalidad entre actividades y riesgos recogido en la legislación vigente.

5. El informe anual previsto en el artículo 25 incluirá, en un apartado específico sobre proporcionalidad, la información relevante sobre lo dispuesto en los apartados anteriores.” (el resaltado es mío).

[1725]

Confr. Daniel Levi, María Shakespear, Luciana Liefeldt y Andrés Schreiber, *¿Qué hay de realmente nuevo en la reciente regulación del BCRA sobre PSP?* publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.

[1726]

Ibid.

[1727]

Ibid.

[1728]

Ibid.

[1729]

Véase <https://www.satoshitango.com/es-AR/>

[1730]

Confr. Fernando Branciforte, *Análisis de las comunicaciones “A” 6859 y “A” 6885 del BCRA. Su implicancia para las empresas Fintech, usuarios y consumidores de sus servicios*, publicado el día Miércoles 19/02/2020 en la Edición Especial: Fintech, del Diario La Ley.

[1731] Ibid.

[1732] Ibid.

[1733] Ibid.

[1734] Confr. <https://binance.zendesk.com/hc/en-us/articles/360017720731> recuperado el 11/05/2020.

[1735] Confr. <https://news.bitcoin.com/binance-denies-400-btc-listing-quote-accuser-responds-you-are-a-fking-liar/> disponible al 11/05/2020.

[1736] Confr. <https://www.newsbtc.com/2018/10/09/worlds-largest-crypto-exchange-binance-delists-4-assets-prioritizes-user-protection/> recuperado el 11/05/2020. En <https://hackernoon.com/altcoins-blacklist-lifting-the-veil-of-secrecy-cb8218750c26> se ha sostenido que “those tokens that are *running low on trade volumes and not active are automatically getting in the risk group (...) ‘scam token’ as not moving on time with tech development schedule and not having a working product.*”

[1737] Confr. <https://binance.zendesk.com/hc/en-us/articles/360017664751-Binance-Listing-Fee-Update> y <https://www.binance.charity> recuperados el 11/05/2020.

[1738] Véase *supra* en notas 144 y 647.

[1739] Confr. <https://cointelegraph.com/explained/erc-20-tokens-explained> recuperado el 11/05/2020. Ampliar en <https://eips.ethereum.org/all>, disponible al 11/05/2020.

[1740] Ampliar en <https://medium.com/@micobo/security-tokens-an-erc-standards-comparison-919e7c379f37> disponible al 11/05/2020. Se afirma allí en relación a los ERCs, que “*this is Ethereum’s version of a “Request for Comments”, which is a type of publication based on the principal technical development and standards-setting bodies for the internet –the Internet Engineering Task Force and Internet Society. So, before an ERC becomes a standard, it has to be approved as Ethereum Improvement Proposal (EIP), evaluated, revised, commented and finally accepted by the community. These ERC documents defining guidelines to help create tokens with a standard set of rules. This is important to ensure compatibility of these tokens with the several wallets and crypto exchanges as well as other smart contracts. Without such standards, developers of exchanges, wallets and other smart contracts would have to write custom code to support each individual token, which overall would require a lot of work and effort that could be avoided. Simply said, these standards make each piece speak the same language and therefore enable them to interact with each other, while at the same time it reduces work for developers and potentially leads to a better and cleaner*

finished code.

So, tokens that are compliant with a standard like ERC20 are supported without the need for any custom code and are therefore instantly monetize- and tradeable. Such standards also allow for developers to easily make use of the technology without doing everything from the scratch. Standards are highly important in order to promote mass adoption of tokens and minimize efforts developing or integrating them in existing DApps.” El resaltado es mío.

[1741]

Una regla obligatoria, quizás la más importante, es la que fija la cantidad de tokens que se crearán, y recordar que cada uno de ellos será divisible hasta por 18 decimales.

[1742]

Esta regla permite que el creador del token sepa cómo están distribuidos sus tokens, cuántos hay depositados en cada llave pública en todo momento. Trazabilidad total. Si recurre a un *Exchange* que aplica normas de KYC-AML, el creador del token puede saber la identidad real a la que pertenece cada llave pública a donde están alojados los tokens creados.

[1743]

Esta función permite transferir los tokens creados entre cuentas, es decir, entre llaves públicas.

[1744]

Esta función chequea y aprueba cada transferencia de un token sólo contra la cantidad total de tokens creados, verificando que no falten ni sobren tokens, y por ende, evita que alguien pueda tener más tokens que los creados.

[1745]

Esta función es la que impide que uno transfiera más tokens que los que tiene acreditados en su cuenta.

[1746]

Si un token puede tener hasta 18 decimales, significa que es divisible hasta esa misma cantidad de veces.

[1747]

Véase <https://polymath.network/erc-1400>

[1748]

Confr. Ampliar en <https://medium.com/@micobo/security-tokens-an-erc-standards-comparison-919e7c379f37> disponible al 11/05/2020. Se afirma en relación al ERC721 que *“is the first Non-Fungible Token standard that is already in final state and used in ICO projects. It is currently most used in (collectible) crypto games to tokenize unique individual assets. This standard provides basic functionality to track and transfer ownership of NFT. Gas costs are slightly lower compared to ERC20. Uses ERC165 to ensure that a contract is compliant with the interface.”*

[1749]

Confr. Kevin Werbach, en *Trust, but verify...* o.c. p. 518.

[1750]

Véase *supra* nota 651.

[1751] Confr. David Morris, *The rise of cryptocurrency Ponzi schemes*, disponible el 11/05/2020 en

<https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/>.

[1752] Véase <https://gnosis.io>

[1753] Confr. David Morris, *The rise of cryptocurrency...o.c.*

[1754] Ibid.

[1755] Confr. Kevin Werbach, en *Trust, but verify... o.c.* p. 519.

[1756] Ibid.

[1757] Idem, p. 520. Afirma el autor citado que “*not all token offerings are necessarily securities, for one thing. An SEC investigation concluded that The DAO tokens should have been classified as securities and therefore subject to the SEC’s rules for public offerings. However, it stopped short of declaring that all tokens would be. **Regulators around the world need to consider how to draw lines around token offerings that protect investors without chilling innovation.** Without such efforts, investors will be hurt. And failures of ICOs could undermine confidence in the market as a whole. Blockchain effectively implements a decentralized security model, but this does not obviate the need for legal and regulatory involvement.*”

[1758] Confr. <https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115>, disponible al 12/05/2020.

[1759] Ibid.

[1760] Confr. Marcelo Corrales, Mark Fenwick, Helena Haapio y Erik Vermeulen, *Tomorrow’s lawyers today? Platform-driven legaltech, smart contracts & the new world of legal design*, publicado en *Journal of Internet Law*, Abril, 2019, p. 3.

[1761] Idem, p. 5.

[1762] Idem, p. 8.

[1763] Ibid.

[1764] Idem, p. 9.

[1765] Ibid.

[1766] Véase <https://creativecommons.org/licenses/>

[1767] Confr. Kevin Conboy, *DIAGRAMMING TRANSACTIONS: SOME MODEST PROPOSALS AND A FEW SUGGESTED RULES*, disponible al 11/05/2020 en <https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1339&context=transactions>.

[1768] Confr. Marcelo Corrales, Mark Fenwick, Helena Haapio y Erik Vermeulen, *Tomorrow's lawyers today? Platform-driven legaltech...o.c.*, p. 9.

[1769] Véase la interesantísima obra de Helena Haapio y Margaret Hagan, *Design Patterns for Contracts*, en Erich Schweighofer y otros (Editores), *Networks. Proceedings of the 19th International Legal Informatics Symposium IRIS 2016*, Ed. Österreichische Computer Gesellschaft OCG, Viena, 2016, pp. 381-388, disponible al 11/05/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747280. Véase también <http://www.legaltechdesign.com/legal-projects-clearinghouse/> disponible al 11/05/2020.

[1770] Confr. CCCN, Art. 1100.

[1771] Confr. Arianna Rossi, Rossana Ducato, Helena Haapio, Stefania Passera y Mónica Palmirani, *Legal design patterns: towards a new language for legal information design*, recuperado el 11/05/2020 en https://stefaniapassera.com/wp-content/uploads/2019/03/preprint_LEGAL-DESIGN-PATTERNS.pdf

[1772] Ibid.

[1773] Ibid.

[1774] Véase <https://www.optimizely.com/optimization-glossary/user-journey-map/> y <https://teston.io/en/blog/user-journey>

[1775] Confr. Arianna Rossi, Rossana Ducato, Helena Haapio, Stefania Passera y Mónica Palmirani, *Legal design patterns: towards a new...o.c.*

[1776] Confr. Luigi Buonanno, *Civil Liability in the Era of New Technology: The Influence of Blockchain* *Blockchain as the Backbone of a New Technology-based Civil Liability Regime*, recuperado el 11/05/2020 en https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/YLA_Award/Subm

[1777] Confr. Luigi Buonanno, *Civil Liability in the Era of New Technology...o.c.*, p. 6.

[1778] Idem, p. 8.

[1779] Idem, p. 9.

[1780] Ibid.

[1781] Idem, p. 10.

[1782] Idem, p. 11.

[1783] Ibid.

[1784] En contra de esta opinión de responsabilizar a los *operadores*, véase Angela Walch, *The bitcoin blockchain as financial market infrastructure: a consideration of operational risk*..o.c. Véase también la opinión citada por Buonanno, o.c., p. 11, nota 43, citando a Josef Esser, *Grundlagen und Entwicklung der Gefährdungshaftung*, 2nd. ed (CH Beck 1961): “**According to Esser, the conscious and voluntary exposure to the risk by the damaged party would always impede strict liability of the latter.**” El resaltado es mío.

[1785] Idem, p. 12.

[1786] Véase en este sentido la Declaración del Parlamento Europeo del 17/02/2017, por la cual se recomiendan ciertas reglas de responsabilidad civil en materia de robots, disponible al 11/05/2020 en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html, apartado 57. En opinión del Parlamento Europeo, “*a possible solution to the complexity of allocating responsibility for damage caused by increasingly autonomous robots could be an **obligatory insurance scheme**, as is already the case, for instance, with cars; notes, nevertheless, that unlike the insurance system for road traffic, where the insurance covers human acts and failures, an insurance system for robotics should take into account all potential responsibilities in the chain.*” El resaltado es mío.

[1787] Idem, p. 13.

[1788] Confr. Robert Schwinger, *Blockchain law: liability rumblings along the blockchain*, disponible al 11/05/2020 en <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/schwinger-nylj-column-blockchain-law.pdf?revision=06c594b5-8d6f-4234-994c-ba39148cc210&la=en>.

[1789] Véase discurso del Presidente de la CFTC, en Octubre de 2018, disponible al 11/05/2020 en <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>.

[1790] Véase <https://cryptonewsovernonsense.substack.com/p/the-berk-case-v-coinbase>, <https://www.ccn.com/coinbase-bitcoin-cash-lawsuit/>, y <https://www.bloomberg.com/news/articles/2019-08-07/coinbase-must-face-negligence-suit-over-bitcoin-cash-launch>, disponibles al 11/05/2020.

[1791] Puede ampliarse en <https://www.theblockcrypto.com/post/35381/fed-court->

[says-coinbase-can-be-held-negligent-for-allowing-dysfunctional-market-and-why-this-matters](#), disponible al 11/05/2020. A la misma fecha, la demanda está disponible en: <https://es.scribd.com/document/421054454/Berk-v-Coinbase>. Para un análisis del insider trading en materia de acciones con oferta pública, véase del autor “*El uso de información privilegiada en el mercado de acciones y la acción de responsabilidad*”, ponencia en co-autoría con los Dres. Leopoldo Godio y Sebastián Vanella Godino, presentada al I [Congreso Argentino Sobre Mercado de Capitales, Aspectos Jurídicos y Contables](#), organizado por UCEMA, publicada en Mercado de Capitales, Aspectos Jurídicos y Contables, Dto. de Finanzas UCEMA, Ed. Osmar D. Buyatti, 2008, págs. 395-409.

[1792] Véase *supra* en § 3.4.2.2.2.

[1793] Véase *supra* en § 2.6.1.

[1794] Confr. Dirk Zetsche, Ross Buckley y Douglas Arner, *The distributed liability of distributed ledgers: legal risks of blockchain*, recuperado el 12/05/2020 en <https://illinoislawreview.org/wp-content/uploads/2018/10/BuckleyEtAl.pdf>.

[1795] *Idem*, p. 1394. Afirman: “Some authors suggest that no contractual relationship exists in distributed networks where the user is unknown and the userbase unstable, where the performance of the service depends on who is connected at what time, and where none of the individual nodes is in itself essential (such as in permissionless blockchains like Bitcoin). Proponents of the idea that the DLT relationship does not give rise to legal rights refer implicitly to participants’ lack of intent to grant contractual rights to co-users. Business entities, however, are often unaware of all participants, and their roles, in complex business interactions. **A distributed ledger is a complex network of users and contractual relationships that may change from time to time depending on who is participating in the ledger operation. While anonymity of the parties renders enforcement potentially difficult, it does not mean that the actions of individuals who together “operate” the distributed ledger are not legally relevant, potentially in a wide range of different jurisdictions.** In a distributed ledger, electronic messages and transactions coincide; any message a node sends is a declaration of intent and contribution to the transaction. It is inconsistent to deny legal relevance of cooperation where **only reliance on others ensures access to, and transfer of, one’s own asset value and where this very cooperation by others is the precondition of contributing to the ledger in the first place (...)** While enforcement may be difficult, we must not confuse potential for legal liability with the challenge of enforcement.

Another argument against contractual liability is that node operators may have no way of knowing to which use their fragmented contribution to the network is put, which, for instance, could include money laundering or terrorist financing. Again, this

argument is flawed. Nodes could require AML/CFT (“Anti-Money Laundering/Combating the Financing of Terrorism”) checks as a precondition for hard currency being exchanged into virtual assets—they could define this as a precondition for the overall use of the networks. The fact that nodes sign up to the network, particularly when they buy/sell/mine Bitcoins, without AML/CFT checks may evidence ignorance of the law but not the law’s inapplicability.”

Los resaltados son míos.

[1796]

Idem, p. 1394, nota 133. Véase *supra* en § 4.3.5.

[1797]

Ibid.

[1798]

Idem, p. 1396.

[1799]

Idem, p. 1398.

[1800]

Idem, p. 1400.

[1801]

Ibid. Afirman los autores citados que “while participation in a clearing and settlement distributed ledger system that relies on all nodes’ mutual cooperation for identifying true transactions may be deemed a joint pursuit of a shared objective sufficient under some civil laws to establish a joint venture, the fee and profit-sharing agreement will determine whether such a blockchain is deemed a partnership under common law. **As long as profit opportunities are held by a third-party distributed ledger sponsor/organizer and the nodes bear their own expenses and are rewarded on a predetermined basis as with Bitcoin, the risk that the system is a partnership at common law is very low indeed.** If in a permissioned blockchain, however, the network of validation nodes offers the services of the network to third-party users which pay “the network” for these services, the system may be deemed a partnership; and in turn, all validation nodes as partners may be liable vis-à-vis third parties (...) the case of the DAO illustrates the potential magnitude of the risk. In the DAO, all investors jointly voted on investment proposals, all investors jointly held the assets acquired, **no legal entity was positioned as a liability shield in between assets and investors, and all investors agreed that they were to share the profits generated by the assets.** If the DAO’s assets had generated losses rather than profits (for instance, if people working in a factory held by the DAO were harmed by an accident) all investors could be held to be partners and personally liable.” El resaltado es mío.

[1802]

Idem, p. 1401. Afirman los autores: “as a rule of thumb, the risk of liability associated with DLT participation based on partnership law increases in the following circumstances: (i) the more a server owner benefits from participating in the distributed ledger through profits (as long as there are others who benefit in the same way); (ii) the greater a server owner’s influence is on the server design, set-up, or

update, with “creators” being more influential than “simple users”; and (iii) the greater the server owner’s influence on the decision to let others use or be excluded from using the distributed ledger.

From the last consideration follows that the function of a **validation node in a permissioned blockchain with a veto right against access or updates (“consortium blockchain”)** is more likely to lead to personal liability than the “simple” mining function in Bitcoin. The result of the former may well not only be mutualization of data processing but also mutualization of liabilities and risks.” El resaltado es mío.

[1803] Véase *supra* en § 3.5.1.8.

[1804] Ley N° 27.442, Art. 58. Cuando las infracciones previstas en esta ley fueren cometidas por una persona jurídica, la multa también se aplicará solidariamente a los directores, gerentes, administradores, síndicos o miembros del Consejo de Vigilancia, mandatarios o representantes legales de dicha persona jurídica que por su acción o por la omisión culpable de sus deberes de control, supervisión o vigilancia hubiesen contribuido, alentado o permitido la comisión de la infracción. En tal caso, se podrá imponer sanción complementaria de inhabilitación para ejercer el comercio de uno (1) a diez (10) años a la persona jurídica y a las personas enumeradas en el párrafo anterior. **La solidaridad de la responsabilidad podrá alcanzar a las personas controlantes cuando por su acción o por la omisión de sus deberes de control, supervisión o vigilancia hubiesen contribuido, alentado o permitido la comisión de la infracción.”**

[1805] Confr. Dirk Zetsche, Ross Buckley y Douglas Arner, *The distributed liability of distributed ledgers: legal risks of blockchain...o.c.*, p. 1404.

[1806] *Idem*, p. 1407.

[1807] Véase el resumen del caso en el comunicado de la SEC disponible al 12/05/2020 en <https://www.sec.gov/litigation/litreleases/2014/lr23090.htm>

[1808] Esta es el endendimiento dado a la expresión: “When a case presents a particular hardship, the court is tempted to vary a generally sound law to avoid the hardship, *resulting in a new law that, though perhaps fine for the case at hand, would be unsound as a general rule of conduct.* This is how most commentators understand the aphorism. For example, Garner’s Dictionary of Legal Usage says the “catchphrase refers to the danger that a decision operating harshly on the defendant may lead a court to make an unwarranted exception or otherwise alter the law” (Garner (2011). Heuston (1978) and Radin (1938), 40-42, say essentially the same thing. Schauer (2006) runs further with the idea, arguing that because cases (not just cases posing a special hardship) are unrepresentative of the range of problems that the law would be called upon to resolve, case-by-case lawmaking makes bad law.” Confr. Sepher

Shahshahani, *Hard cases make bad law? A theoretical investigation*, disponible al 13/05/2020 en <https://pdfs.semanticscholar.org/96a0/c3aab8d72dce469974f3199407357fd7d028.pdf?ga=2.89281432.2057681739.1589381031-309015164.1589381031>, p. 5.

[1809] Ibid.

[1810] Confr. Luciano Minetti Kern, *El perfil del Juez a partir de la entrada en vigencia del Código Civil y Comercial. Nuevos desafíos y razones para dejar atrás prácticas disvaliosas. Hacia un Juez Constitucional*, recuperado el 13/05/2020 en <http://servicios.jusrionegro.gov.ar/inicio/comunicacionjudicial/index.php/especiales/itperfil>

[1811] Confr. Sepher Shahshahani, *Hard cases make bad law? A theoretical investigation...o.c.*, p. 6.

[1812] La demanda de la SEC contra Shavers y su fideicomiso, al 12/05/2020, está disponible en <https://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf>

[1813] Idem, apartado 4.

[1814] Idem, apartado 15. En sus publicidades online, Shavers afirmaba que: “My clients deal in cash only and I don’t move a single coin until the cash is in hand and I’m out of harms [sic] way (just in case :)). So risk is almost 0.”

[1815] Confr. <https://www.reuters.com/article/us-bitcoin-fraud-texas/texan-gets-one-and-a-half-years-in-prison-for-running-bitcoin-ponzi-scheme-idUSKCN1012W8>, disponible al 12/05/2020.

[1816] Idem, apartado 27.

[1817] Idem, apartados 29, 34.

[1818] Confr. <https://www.reuters.com/article/us-bitcoin-fraud-texas/texan-gets-one-and-a-half-years-in-prison-for-running-bitcoin-ponzi-scheme-idUSKCN1012W8>, disponible al 12/05/2020.

[1819] Al 15/05/2020, el pedido de orden de cese está disponible en <https://www.sec.gov/litigation/admin/2017/33-10445.pdf>

[1820] Ibid.

[1821] Ibid.

[1822] Ibid.

[1823] Confr. <https://www.sec.gov/news/press-release/2017-227>, disponible al 15/05/2020.

[1824] Al 13/05/2020, la demanda de la SEC está disponible en <https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf>

[1825] Ibid, apartados 3 y 4.

[1826] Confr. <https://www.sec.gov/news/press-release/2018-280> disponible al 13/05/2020.

[1827] Confr. <https://www.cftc.gov/PressRoom/PressReleases/pr7675-18> disponible al 13/05/2020.

[1828] Confr. apartado II de la sentencia que se encuentra disponible, al 13/05/2020 en <https://casetext.com/case/commodity-futures-trading-commn-v-mcdonnell>

[1829] Confr. <https://www.cftc.gov/PressRoom/PressReleases/7774-18> disponible al 13/05/2020.

[1830] Confr. sentencia del caso, disponible, al 13/05/2020 en <https://casetext.com/case/commodity-futures-trading-commn-v-mcdonnell>

[1831] Al 13/05/2020, la sentencia está disponible en <http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0264&lang1=es&lang2=EN&type=TXT&ancre=>

[1832] Idem, apartado 12.

[1833] Idem, apartado 13.

[1834] Idem, apartado 57.

[1835] Se sigue en este apartado la exposición de Federico Ossola y Aldo Azar, en Tratado de Derecho Civil y Comercial, Andrés Sánchez Herrero (Director) y Pedro Sánchez Herrero (Coordinador), Ed. Thompson Reuters La Ley, Tomo III, Buenos Aires, 2016, p. 737.

[1836] Ibid.

[1837] Idem, p. 739.

[1838] Ibid.

[1839] Idem, p. 740.

[1840] Idem, p. 741.

[1841] Ibid.

[1842] Ibid.

[1843] Art. 1757, CCCN.- “Hecho de las cosas y actividades riesgosas. Toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención.”

[1844] Art. 1722, CCCN.- “Factor objetivo. El factor de atribución es objetivo cuando la culpa del agente es irrelevante a los efectos de atribuir responsabilidad. En tales casos, el responsable se libera demostrando la causa ajena, excepto disposición legal en contrario.”

[1845] Art. 1758, CCCN.- “Sujetos responsables. El dueño y el guardián son responsables concurrentes del daño causado por las cosas. Se considera guardián a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella. El dueño y el guardián no responden si prueban que la cosa fue usada en contra de su voluntad expresa o presunta. En caso de actividad riesgosa o peligrosa responde quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros, excepto lo dispuesto por la legislación especial.”

[1846] Idem, p. 743.

[1847] Ibid.

[1848] Confr. Art. 1521.- Responsabilidad por defectos en el sistema. El franquiciante responde por los defectos de diseño del sistema, que causan daños probados al franquiciado, no ocasionados por la negligencia grave o el dolo del franquiciado.

[1849] Art. 6º, Ley N° 24.240 — Cosas y Servicios Riesgosos. Las cosas y servicios, incluidos los servicios públicos domiciliarios, cuya utilización pueda suponer un riesgo para la salud o la integridad física de los consumidores o usuarios, deben comercializarse observando los mecanismos, instrucciones y normas establecidas o razonables para garantizar la seguridad de los mismos. En tales casos debe entregarse un manual en idioma nacional sobre el uso, la instalación y mantenimiento de la cosa o servicio de que se trate y brindarle adecuado asesoramiento. Igual obligación regirá en todos los casos en que se trate de artículos importados, siendo los sujetos anunciados en el artículo 4 responsables del contenido

de la traducción.

[1850] Idem, p. 746. Citan los autores como ejemplos a las Leyes N° 24.051 de residuos peligrosos y N° 24.804, de actividad y daños nucleares.

[1851] Ibid.

[1852] Idem, p. 748.

[1853] Idem, p. 761.

[1854] Idem, p. 762.

[1855] Confr. Art. 176, Ley N° 20.744 —Tareas penosas, peligrosas o insalubres. Prohibición.

Queda prohibido ocupar a mujeres en trabajos que revistan carácter penoso, peligroso o insalubre.

La reglamentación determinará las industrias comprendidas en esta prohibición.

Regirá con respecto al empleo de mujeres lo dispuesto en el artículo 195.

Los autores citan también como ejemplos de tal calificación legal de actividad riesgosa o peligrosa: los riesgos del trabajo, de la contaminación ambiental, de la organización de espectáculos públicos, de la actividad nuclear, del transporte de mercaderías y personas.

[1856] Idem, p. 763.

[1857] Ibid.

[1858] Idem, p. 765.

[1859] Idem, p. 765.

[1860] Idem, p. 767.

[1861] Ibid.

[1862] Idem, p. 768.

[1863] Idem, p. 769.

[1864] Idem, p. 753.

[1865] Idem, p. 771.

[1866] Idem, p. 772. Afirman Ossola y Azar que en el Código Civil Francés y en el Código del Consumo Italiano, el empresario no debe responder si el defecto es debido

a la conformidad del producto *con las reglas imperativas de orden legislativo o reglamentario, o por alguna medida vinculante*. En nuestro derecho, afirman, tal eximente sería válida como causa ajena por el hecho del Príncipe, que obliga a elaborar la cosa con el defecto, o que prohíbe que ésta tenga las medidas de seguridad que la haría idónea para prevenir los daños.

[1867] Idem, p. 438.

[1868] Ibid.

[1869] Ibid.

[1870] Ibid.

[1871] Véase *supra* en § 3.5.1.

[1872] Véase *supra* en § 3.3.1.1.

[1873] Confr. Resol. N° 15, del 31/01/2019, por la que se aprueba la formalización de la Mesa de Innovación de Financiera del BCRA, recuperado el 8/05/2020 en <http://www.bcra.gov.ar/Pdfs/Institucional/Transparencia%20activa/E-F-RD001519.pdf>

[1874] Confr. http://www.bcra.gov.ar/Pdfs/Noticias/Innovacion_Financiera_Bases_2018.pdf recuperado el 10/05/2020.

[1875] Confr. <https://www.asiafundmanagers.com/int/chinas-plans-for-a-digital-yuan/> disponible al 10/05/2020.

[1876] Confr. http://www.bcra.gov.ar/Pdfs/Noticias/Innovacion_Financiera_Bases_2018.pdf recuperado el 10/05/2020.

[1877] Confr. <http://www.bcra.gov.ar/Pdfs/Noticias/Bases%20y%20Condiciones%20PIF%202019.pdf> recuperado al 12/05/2020.

[1878] Confr. <https://es.cointelegraph.com/news/argentinas-central-bank-boosts-poc-based-on-blockchain-technology> recuperado al 12/05/2020. Se afirma que en este sistema –en fase de prueba- los distintos actores del sistema financiero podrán acceder libremente y se espera que cursen de manera automática, confiable y segura a los reclamos y podrán darle curso de manera tal que podrán tener la trazabilidad desde el inicio del reclamo hasta la solución del mismo y de igual manera obtener información en tiempo real sobre las novedades de cuentas bancarias ingresados al sistema.

[1879] Ibid., p. 53.

[1880] Confr. <https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1332/1332grupo-de-trabajo-fintech> recuperado al 8/01/2020.

[1881] Véase *supra* en § 4.5.13.

[1882] Ley N° 24.144, Art. 47. “*Son facultades del superintendente: (...) f) Aplicar las disposiciones legales que sobre el funcionamiento de las denominadas tarjetas de crédito, tarjetas de compra, dinero electrónico u otras similares, dicte el Honorable Congreso de la Nación y las reglamentaciones que en uso de sus facultades dicte el Banco Central de la República Argentina.*”

[1883] Confr. Eduardo Barreira Delfino, *Bancos y entidades financieras*, en Eduardo Favier Dubois (H) (Director), Ignacio Alterini (Coordinador), *Manual de Derecho Comercial*, Ed. Thomson Reuters La Ley, Buenos Aires, 2016, p. 745.

[1884] Ibid.

[1885] Idem, p. 747. Señala Barreiro Delfino que la regulación y supervisión de los mercados financieros es un desafío global dada la globalización financiera, con lo cual se han creado normas que operan como principios básicos para una supervisión bancaria efectiva, adoptados por todos los bancos centrales. Se trata de las Normas de Basilea cuyo dictado se inició en 1988, y ya cuenta con tres revisiones. Basilea III fue producto de la última crisis financiera de 2007-2011, que también dio nacimiento a Bitcoin.

[1886] Idem, p. 747.

[1887] Idem, p. 746.

[1888] Idem, p. 747.

[1889] Idem, p. 749.

[1890] Ibid.

[1891] Ibid.

[1892] Idem, p. 750.

[1893] El capital inicial del BCRA fue repartido 2/3 para el sector privado y 1/3 para el sector público, procurándose su *actuación independiente*. Debates parlamentarios de la época albergan tesoros de la cultura y la futurología, como estas palabras de Nicolás Repetto “*..vamos a ver más adelante, como el peligro más serio para un Banco Central*

lo constituye el Estado. Es el Estado con su necesidad permanente de dinero, con su déficit continuo, el enemigo más terrible del Banco Central”. Citado por Barreira Delfino, o.c., p. 751.

[1894] Confr. Cámara Argentina de la Construcción, *Historia de la inflación Argentina*, recuperado el 13/05/2020 en https://www.cac.com.ar/data/documentos/10_Historia%20de%20la%20inflación%20er

[1895] Confr. Eduardo Barreira Delfino, *Bancos y entidades financieras*, en Eduardo Favier Dubois (H) (Director)...o.c., p. 756.

[1896] Idem, p. 760. Sostiene Barreira Delfino que la empresa bancaria debe gestionar diversos riesgos: de liquidez, de tasas de interés, de moneda, de mercado, y operacional y legal.

[1897] Idem, p. 757.

[1898] Idem, p. 763. Aclara Barreiro Delfino que los recursos financieros no son sólo la moneda corriente, de curso legal, o fiduciaria, sino también aquéllos bienes de rápida y fácil convertibilidad en dinero, como los depósitos en caja de ahorro, los certificados a plazo fijo transferibles o intransferibles, los papeles de comercio negociables y los títulos de endeudamiento público o privados.

[1899] El CCCN regula los contratos bancarios en el Libro III, Título IV, Capítulo XII.

[1900] Idem, p. 767.

[1901] Idem, p. 768.

[1902] Confr. Sean Ross, *Should commercial and investment Banks be legally separated?* Disponible al 19/05/2020 en <https://www.investopedia.com/ask/answers/032715/should-commercial-and-investment-banks-be-legally-separated.asp>. Para una contundente argumentación en el sentido que se postula, véase en general el pensamiento del Nobel de Economía Joseph Stiglitz, y su opinión en <https://www.cnbc.com/2010/01/19/us-does-not-have-capitalism-now-stiglitz.html>, disponible al 19/05/2020.

[1903] Véase información pública disponible en https://www.bcra.gov.ar/SistemasFinancierosYdePagos/Entidades_financieras.asp

[1904] Se sigue la exposición del artículo –debidamente actualizado– del autor, *La negociación bursátil de cheques de pago diferido*, publicado en Erreius, Compendio Jurídico, tomo 37, año 2010, Enero-Febrero, p. 189 y siguientes.

[1905] Casi una década después, en Julio de 2019, el uso de cheques de pago diferido

para negociación bursátil había crecido un 110% comparado a un año antes. Confr. <https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1352/1352financiamiento-en-el-mercado-de-capitales-agosto-2019>, recuperado el 15/05/2020.

[1906]

Confr. Art. 54, Ley 24.452 (B.O. 2/3/95), según modificación introducida por Ley 24.760 (B.O. 31/7/97).

[1907]

Confr. el Dto. 1387/2001, en su art. 5, sustituyó el régimen de endosos hasta ese entonces vigente. Hasta ese momento la regulación de la Ley N° 24.452 estipulaba, en su art. 12, que el cheque extendido a favor de una persona determinada con la cláusula "*no a la orden*" no era transmisible (sic, endosable) sino bajo la forma y con los efectos de una cesión de créditos. Dicho principio recibió una primera excepción con la modificación de marras, que permitió que por simple endoso el cheque fuera transferido a favor de una entidad financiera comprendida en la Ley N° 21.526 (a los fines de su descuento). Naturalmente, de modo lateral a éste descuento en el sistema financiero "formal" y mucho antes, apareció un descuento "informal", con menores requisitos pero tasas más altas.

[1908]

En orden a permitir la operatoria, el citado Dto. 386/03 introduce dos modificaciones en la Ley N° 24.452. Por un lado, modifica nuevamente el Art. 12, y permite que por simple endoso un cheque se transfiera mediante depósito a Caja de Valores S.A. (CVSA) para su posterior negociación en Mercados de Valores. Por otro lado, modifica el Art. 56, norma específica del Capítulo XI, "Del cheque de pago diferido". Con la redacción actual, el Art. 56 admite la negociación de los CHPD en las Bolsas y Mercados del país. Sin embargo, expresamente declara que la oferta primaria y negociación secundaria de CHDP no es considerada oferta pública, por lo que los endosantes o cualquier otro firmante no quedan sujetos al régimen de emisores o intermediarios que preveía, por aquél entonces, la Ley 17.811. En cuanto a la función de Caja de Valores S.A., el depósito de los CHPD no le transfiere ni la propiedad ni el uso, debiendo CVSA conservarlos, custodiarlos y efectuar las operaciones y registraciones contables que deriven de su negociación. Mientras el endoso a su favor lo sea a los fines de su negociación, no queda obligada al pago, ni es responsable por los defectos formales de los documentos, ni la legitimación de los firmantes o autenticidad de las firmas. Finalmente, el Dto. dispone que la negociación bursátil no genera obligación cambiaria entre las partes intervinientes en la operación.

[1909]

Lo que hizo dictando la Comunicación "A" 4010, de fecha 5/9/03, que incorpora el punto 4.5, intitulado "Negociación bursátil", a la Sección 4 de la "Reglamentación de la cuenta-corriente bancaria".

[1910]

Reglamentación aprobada por el Consejo de la BCBA, y presentada a la CNV para su conformidad el 31/10/03, siendo aprobada el 20/11/03 mediante Resolución

14.689. Cabe destacar que la reglamentación dada por la Bolsa de Buenos Aires inicialmente contemplaba la negociación *directa* de CHPD, mas ésta misma no fue aprobada por la CNV sino hasta el 23/06/05, mediante Resolución General 480/2005. En el caso de Córdoba, su "Reglamento para la cotización de cheques de pago diferido" fue aprobado por la CNV mediante Resolución 15.062, del 28/4/05.

[1911]

Mediante Circular 3502, del 19/12/03, emitida por el Directorio del Merval y Circular 722, del 22/08/05, emitida por el Directorio del MVC.

[1912]

En junio de 2005, la CNV dicta la Resolución General 480/2005, autorizando la negociación directa de CHPD, que había sido una modalidad admitida por Resolución 2/2003 de la Bolsa de Buenos Aires. Dicha RG 480/2005 establece las condiciones que debería respetar, hace 15 años, la reglamentación a ser implementada por las Bolsas y Mercados.

[1913]

Merece resaltarse que en la operatoria patrocinada, tal cual originariamente fuese diseñada, las libradoras de los CHPD podían sólo ser: sociedades comerciales legalmente constituidas, cooperativas, asociaciones civiles, mutuales y fundaciones. En el año 2009, la CNV, mediante la Resolución 556, ha ampliado el scope de las libradoras, alcanzando en la actualidad a la Nación, las Provincias, las Municipalidades, los entes autárquicos y las empresas del Estado.

[1914]

Confr. <https://www.cronista.com/finanzasmercados/Las-pymes-se-financiaron-en-el-mercado-por-un-record-historico-durante-mayo-20190604-0022.html> , disponible al 03/05/2020.

[1915]

Confr. <https://www.cnv.gov.ar/SitioWeb/Informes> disponible al 15/05/2020.

[1916]

Se sigue, en general, la exposición del artículo de autor, *Un útil instrumento para el financiamiento PYME: el pagaré bursátil*, publicado en la revista TEMAS DE DERECHO COMERCIAL, EMPRESARIAL Y DEL CONSUMIDOR de Ed. Errepar, Colección Compendio Jurídico, Agosto/2016.

[1917]

La *Ley PYME* modificó: (1) la Ley N° 25.300 de Fomento para la Micro, Pequeña y Mediana Empresa; (2) la Ley N° 25.413 de Competitividad; (3) la Ley N° 11.683 de Procedimiento Fiscal; (4) la Ley N° 24.467 de Pequeña y Mediana Empresa; (5) la Ley N° 22.317 de Régimen de Crédito Fiscal del Instituto Nacional de Educación Tecnológica; (6) la Ley N° 23.576 de Obligaciones Negociables; (7) la Ley N° 20.091 de Entidades de Seguros; y (8) el Decreto-Ley 5.965 de Letra de Cambio y Pagaré.

[1918]

El Título II de la *Ley PYME*—compuesto por los artículos 4 a 11— introdujo una batería de reformas, entre las que cabe destacar: (i) la creación de un régimen impositivo especial para las Micro, Pequeñas y Medianas Empresas, a las que se

excluye —a partir del ejercicio fiscal que iniciaba el 01/01/2017— del impuesto a la ganancia mínima presunta; (ii) permite computar —total o parcialmente, según la dimensión de la empresa— el impuesto sobre los créditos y débitos en cuentas bancarias y otras operatorias, como pago a cuenta del impuesto a las ganancias —sea al momento de presentar la declaración jurada anual del impuesto, o antes de esto al momento de pagarse sus anticipos—; (iii) permite diferir el pago del impuesto al valor agregado hasta el vencimiento del segundo mes inmediato siguiente al de su vencimiento original; (iv) se instruye a A.F.I.P. para que establezca un procedimiento simplificado de ventanilla única para el pago de impuestos nacionales; y (v) fija beneficios impositivos diferenciales para Micro, Pequeñas y Medianas Empresas que operen en economías regionales, beneficio que tendrá como mínimo un 5% y como máximo un 15% con relación a empresas que no operen en economías regionales.

[1919]

La Ley PYME creó un régimen transitorio de fomento para las inversiones productivas realizadas por Micro, Medianas y Pequeñas Empresas que tengan un track record, y que incorporen bienes de capital nuevos o usados —excepto automóviles— amortizables en el impuesto a las ganancias, y obras de infraestructura. Hasta el 31/12/2018, gozarían de estabilidad fiscal respecto de todos los tributos nacionales directos, tasas y contribuciones, en tanto no disminuyan el nivel de empleo durante al menos dos ejercicios fiscales. Provincias y municipios pueden adherir expresamente, y también acordar estabilidad fiscal en los ámbitos de su poder fiscal.^[1919] En esencia, el estímulo a la inversión productiva se materializaba en dos medidas importantes: (i) el 10% del monto así invertido podrá ser computado como pago a cuenta contra el impuesto a las ganancias que corresponda pagar, siempre que el importe resultante (i.e., 10% del monto invertido) no supere el 2% —se eleva al 3% para industrias manufactureras— del promedio de ingresos netos por ventas registradas en el ejercicio fiscal anterior y en el ejercicio en que se efectúe la inversión; y (ii) los créditos fiscales en el impuesto al valor agregado originados por dichas inversiones productivas —representados en un bono fiscal intransferible— podrán ser imputados al pago de impuestos nacionales, incluidos impuestos aduaneros.

[1920]

En efecto, el FOGAPYME —que antes sólo podía ofrecer garantías directas a favor de entidades financieras bajo supervisión del BCRA sin que éstas garantías superasen el 25% del total de garantías ofrecidas—, podría, a partir de la Ley PYME emitir garantías sin límite, y a favor tanto bancos como de entidades no financieras que operen en el sector MiPyME, y a favor de inversores bursátiles de instrumentos que tengan oferta pública. Por otro lado, se modificó también el Art. 3 de la Ley N° 24.467. Este espíritu "articulador" e "integrador" se aprecia claramente en los Art. 41 de la Ley PYME (que modifica el Art. 34 de la Ley N° 25.300), al disponerse que el régimen de bonificación de tasas de interés para préstamos para Micro, Medianas y Pequeñas Empresas incluirá préstamos con tasas "ya bonificadas" por programas

provinciales o municipales; y en el Art. 42 de la Ley PYME (que modifica el Art. 3 de la Ley N° 24.467), al crearse un régimen de bonificación de tasas de interés para MyPyMEs localizadas en las provincias comprendidas en el Plan Belgrano, o en regiones donde el desempleo sea mayor a la media nacional, o el producto bruto geográfico sea inferior a la media nacional.

[1921]

El Art. 50 de la Ley PYME dispone que la Superintendencia de Seguros de la Nación establecerá los porcentajes mínimos obligatorios que las aseguradoras deberán colocar en instrumentos de financiamiento de capital de trabajo destinado a MiPyMEs tales como cheques de pago de diferido, pagarés, y en fondos comunes de inversión PYME regulados por la Comisión Nacional de Valores.

[1922]

Confr. Ley N° 26.831, Art. 1, inc. c), Arts. 16 y 36. Se autoriza a la CNV a fijar topes a los aranceles y derechos que cobran los mercados autorizados cuando el emisor sea una pequeña o mediana empresa.^[L]_[SEP] Ordinariamente, este comité de auditoría debe integrarse con un mínimo de tres miembros del directorio, dos de los cuales deben ser independientes, tanto de la sociedad como del grupo de control, y no desempeñar tareas ejecutivas en la sociedad. Las PyMEs están exentas de formar dicho Comité, confr. Normas de la CNV T.O. 2013, Título II, Capítulo VI, Sección I, Art. 11.^[L]_[SEP]

[1923]

Confr. Normas de la CNV T.O. 2013, Título II, Capítulo VI "Pequeñas y Medianas Empresas", compuesto por tres Secciones.

[1924]

Confr. CNV, RG N° 743/18, en <https://aif.cnv.gov.ar/descargas/marcoregulatorio/blob/11fef2d6-3f0b-4495-9765-1497c8febefa> recuperado el 18/05/2020.^[L]_[SEP]

[1925]

Confr. Normas de la CNV T.O. 2013, Título II, Capítulo VI, Sección II, Art. 12. Queda bajo responsabilidad de los agentes de negociación verificar que el comprador sea efectivamente un inversor institucional, y éste debe acreditar que la decisión de compra ha sido adoptada de manera independiente.^[L]_[SEP] Por su parte, la Ley N° 27.264 dispone que CNV determinará las obligaciones de los agentes de depósito colectivo en punto a la validación de la información inserta en el pagaré, así como la verificación del cumplimiento de los aspectos formales, sin que pueda ser considerado obligado cambiario.^[L]_[SEP]

[1926]

Confr. Normas de la CNV T.O. 2013, Título II, Capítulo VI, Sección III, Art. 18, inc.18).

Si la deuda emitida prevé un plazo de amortización de hasta 1 año, puede presentarse un *prospecto especial* dispuesto por CNV, y si la emisión se limita exclusivamente a este tipo de deuda corta, la emisora PYME no está obligada a presentar estados

contables trimestrales, y en su lugar, dentro de los 50 días corridos de cerrado cada trimestre, presentarán un estado de movimiento de fondos, un cuadro de estructura patrimonial, un cuadro de estructura de resultados, y las explicaciones necesarias para su

interpretación, todo ello suscripto por el Presidente de la emisora, y acompañado de un informe de revisión limitada de auditor externo y del órgano de fiscalización, debidamente aprobado por el órgano de administración. Confr. Normas de la CNV T.O. 2013, Título II, Capítulo V, Sección VII, Art. 65.

[1927]

Confr. Normas de la CNV T.O. 2013, Título IV. El Régimen PYME CNV libera a las emisoras PYME de presentar sus estados financieros confeccionados según la R.T. N° 26 de la F.A.C.P.C.C., que dispone la adopción de las normas NIIF.^[1]_[SEP]

[1928]

Confr. nota publicada en Cronista Comercial, edición del 23/10/15, disponible al 12/05/2020 en el siguiente link: <http://www.cronista.com/finanzasmercados/Debuto-pagare-bursatil-y-apuntan-a-que-Pymes-estiren-plazos-de-financiacion-20151023-0046.html>

[1929]

La reglamentación de este instrumento exige: (1) que sean emitidos por PYMEs sin indicación del beneficiario, por un monto no menor a \$100.000,00, con cláusula sin protesto. Pueden librarse en moneda extranjera —lo que no se permite en cheques de pago diferido—; (2) Su vencimiento sea posterior a los 180 días desde su libramiento, no excediendo los 3 años; y (3) Estén avalados por S.G.R. o por fondos de garantía públicos registrados ante el B.C.R.A. De acuerdo a la regulación actual del pagaré bursátil, éstos se depositan —sin necesidad de endoso— ante una entidad de depósito autorizada por CNV, quien debe anotar en cuenta las sucesivas transferencias. Como es propio y habitual de la negociación bursátil, no existe responsabilidad por el pago originada en transferencias intermedias, dado que la solidaridad cambiaria sólo "enlaza" al creador del pagaré, a los avalistas y al inversor, según lo dispuesto en el Art. 53 de la Ley N° 27.264, al modificar el Art. 103 del Decreto-Ley 5.965/63, e incorporar un nuevo inciso h), donde expresamente se establece que la negociación bursátil sólo genera obligación cambiaria entre el emisor y el inversor que tenga derechos sobre el pagaré.

[1930]

Esto es sin perjuicio del trámite de Solicitud de Registro en el Régimen PYME CNV e Ingreso a la Oferta Pública que previamente deberá haber realizado la PYME libradora del pagaré bursátil.^[1]_[SEP]

[1931]

Confr. <https://www.cnv.gov.ar/SitioWeb/Informes> disponible al 15/05/2020.

[1932]

Se sigue la exposición del autor en *Cheque electrónico. Nueva reglamentación*, publicado en Erreius On Line, Julio de 2019, cita on line: IUSDC286754A

[1933]

En lo que atañe a datos que debe contener la CAC, estos son: Código de visualización, Fecha y hora de emisión del certificado, tipo de cheque, Entidad financiera girada, Número de sucursal, Número de orden, Domicilio de pago, Creación: lugar, fecha y hora, Fecha de exigibilidad, Beneficiario original, Moneda, Importe a pagar, Importe a pagar, en letras, Número de cuenta corriente, Denominación de fantasía de la cuenta, Cruzado especial para entidad. Beneficiario que lo registra (nombre completo/razón social y CUIT), Cruzado general. Beneficiario que lo registra (nombre completo/razón social y CUIT), Para acreditar en cuenta. Beneficiario que lo registra (nombre completo/razón social y CUIT), Cláusula no negociable. Beneficiario que lo registra (nombre completo/razón social y CUIT), No a la orden. Beneficiario que lo registra (nombre completo/razón social y CUIT), Cheque certificado. Entidad certificante. Fecha de caducidad certificación. Firmantes., Para su negociación en Mercados de Valores, Imputación, Titular de la cuenta: nombre o razón social, identificación tributaria o de identidad y domicilio, Firmante: nombre o razón social, identificación tributaria o de identidad y carácter, ^[L]_[SEP] Endosante: nombre o razón social, identificación tributaria o de identidad, domicilio, fecha y hora del endoso, tipo de endoso (en procuración, no es garante de pago, prohíbe nuevos endosos, para su negociación en mercados de valores y tiene imputación) y entidad gestora responsable del endoso, Avalista: nombre o razón social, firmante, carácter, identificación tributaria o de identidad, domicilio, importe avalado, sujeto avalado, fecha del aval y entidad depositaria del aval, Fecha y hora de presentación al cobro, ^[L]_[SEP] Entidad financiera de presentación al cobro, número y denominación de la sucursal, ^[L]_[SEP] Tenedor que presenta al cobro e identificación tributaria o de identidad, ^[L]_[SEP] Fecha del rechazo, Rechazo parcial y saldo impago, ^[L]_[SEP] Motivos del rechazo, Entidad financiera que suscribe el rechazo, Pagador: nombre o razón social, identificación tributaria o de identidad, Fecha y hora del pago, ^[L]_[SEP] Motivo del pago, Entidad financiera/gestora que informa el pago y Datos de los dos funcionarios firmantes de la entidad financiera emisora. ^[L]_[SEP]

[1934]

Puede ampliarse sobre la operatoria y tipos de *factoring* en la obra del autor, *La regulación de los contratos de fideicomiso, leasing y factoraje en el Código Civil y Comercial de la Nación*, en Revista Argentina de Derecho Empresario, Universidad Austral, Número 16, Septiembre de 2016.

[1935]

La reglamentación de la operatoria de FCE está contenida en la Resolución General N° 780/2019, disponible en <https://www.argentina.gob.ar/normativa/nacional/resolución-780-2019-318603/texto> al 15/05/2020.

[1936]

Confr.

<https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1348/1348financiamiento-en-el-mercado-de-capitales---julio-2019>, disponible al 15/05/2020.

[1937]

Véase, del autor, *Impulso asegurador para la industria de la construcción con la securitización hipotecaria*, disponible al 15/05/2020 en <https://comercioyjusticia.info/blog/opinion/impulso-asegurador-para-la-industria-de-la-construccion-con-la-securitizacion-hipotecaria/>.

[1938]

Véase, del autor, *Financiación de la construcción con “preventas” y “préstamos puente”*, disponible al 15/05/2020 en <https://comercioyjusticia.info/blog/opinion/financiacion-de-la-construccion-con-preventas-y-prestamos-puente/>. Véase también, del autor, *Facilitar el acceso al financiamiento intermedio y potenciar la construcción de viviendas sociales*, disponible al 15/05/2020 en <https://comercioyjusticia.info/blog/opinion/facilitar-el-acceso-al-financiamiento-intermedio-y-potenciar-la-construccion-de-viviendas-sociales/>

[1939]

Se sigue en este apartado, en general, la exposición de Marcelo Camerini, *Funcionamiento e instituciones del mercado de capitales*, en Eduardo Favier Dubois (H) (Director), Ignacio Alterini (Coordinador), *Manual de Derecho Comercial*, Ed. Thomson Reuters La Ley, Buenos Aires, 2016, p. 787.

[1940]

Ibid.

[1941]

También llamado *mercado primario*, es aquél mercado financiero en el que se emiten títulos valores por primera vez, creados al efecto. La relación en este mercado es *directa* entre el emisor que requiere fondeo y el inversor que tiene un excedente de liquidez.

[1942]

También llamado *mercado secundario*, es un mercado de *reventa*, que le permite al inversor que adquirió títulos en el mercado primario darse vuelta y revender el título para recuperar liquidez. El mercado secundario es lo que hace atractivo el mercado primario. Dependiendo de cómo opera el mercado secundario, suele influir en el diseño de bases y condiciones de nuevas emisiones en el mercado primario. El mercado primario establece el volumen de operaciones, y el mercado secundario refleja la liquidez.

[1943]

Ibid.

[1944]

Idem, p. 788.

[1945]

La Ley N° 26.831 en su Art. 2 define al *Mercado de Capitales* como el *ámbito* donde se ofrecen públicamente valores negociables u otros instrumentos previamente autorizados para que, a través de la negociación por agentes habilitados, el público realice actos jurídicos, todo ello bajo la supervisión de la Comisión Nacional de

Valores.

[1946] Idem, 790.

[1947] Idem, p. 794.

[1948] Idem, p. 795.

[1949] La Ley N° 26.831 en su Art. 2 define a la *Oferta Pública* como una *invitación* que se hace a personas en general o a sectores o a grupos determinados para realizar cualquier acto jurídico con valores negociables, efectuada por los emisores, por sus tenedores o por organizaciones unipersonales o sociedades dedicadas en forma exclusiva o parcial al comercio de aquéllos, por medio de ofrecimientos personales, publicaciones periodísticas, transmisiones radiotelefónicas, telefónicas o de televisión, proyecciones cinematográficas, colocación de afiches, letreros o carteles, programas, medios electrónicos incluyendo el uso de correo electrónico y redes sociales, circulares y comunicaciones impresas o cualquier otro procedimiento de difusión.

[1950] La Ley N° 26.831 en su Art. 2 define a los *Mercados* como sociedades anónimas autorizadas por la Comisión Nacional de Valores con el objeto principal de organizar las operaciones con valores negociables que cuenten con oferta pública, quedando bajo competencia del citado organismo las actividades afines y complementarias compatibles con el desarrollo de ese fin.

[1951] Idem, p. 796.

[1952] Idem, p. 802.

[1953] Idem, p. 805.

[1954] Idem, p. 807.

[1955] Señala Camerini, o.c. p. 809 que los AN son personas jurídicas autorizadas por CNV para actuar como intermediarios en los mercados autorizados por CNV. Pueden actuar en la colocación primaria y en la negociación secundaria a través de los sistemas informáticos de negociación de los mercados autorizados por la CNV, tanto para cartera propia, como para terceros clientes. Deben tener un patrimonio neto mínimo. Operan a través de órdenes ingresadas al sistema informático implementado por los mercados autorizados, que registra toda orden ingresada por un AN, dejando constancia del día, la hora, minutos y segundos, especie de valor negociable, precio, y cliente, en otros aspectos. Deben llevar un sistema contable propio, con ciertos libros obligatorios, diferenciándose las operaciones que hacen por cuenta ajena y las operaciones que hacen por cuenta propia. Los AN deben cumplir la normativa de KYC-AML respecto de sus clientes.

[1956]

Señala Camerini, o.c. p. 812 que son personas jurídicas que, por regla, pueden desarrollar todas las actividades de los AN, y además intervenir en la liquidación y compensación de operaciones. Existen dos subcategorías: ALyC integral y ALyC propio. Los primeros pueden ofrecer servicios de liquidación y compensación tanto en colocación primaria como en negociación secundaria a otros ANs. El ALyC propio sólo liquidan y compensan operaciones propias, sean de cartera propia o para sus clientes. Deben tener un patrimonio neto mínimo, que es 15 veces el exigido para un AN en casos de ALyC Integral, y 3,5 veces en caso de ALyC propio.

Los ALyC, a diferencia de los AN, pueden recibir y custodiar fondos o títulos de clientes propios, de otros ANs y de sus clientes. Los ALyCs deben mantener separados sus fondos y títulos valores propios, de los fondos y títulos valores de sus propios clientes, de otros ANs y de sus clientes. No pueden disponer de fondos o títulos de sus clientes sin previa autorización de éstos. Tampoco pueden realizar operaciones que impliquen concesión de financiamiento, préstamo o adelantos a sus clientes propios, a ANs o a clientes de ANs, ni siquiera a través de cesión de derechos. Deben aplicar, tanto respecto de sus clientes como respecto de los clientes de los ANs a los que presten servicios, las normas de KYC-AML. Finalmente, los ALyCs deben cumplir con los requerimientos de márgenes y garantías impuestos por los Mercados o Cámaras Compensadoras. Deben también llevar ciertos libros obligatorios en los que registran las órdenes de sus clientes y también las propias.

[1957]

Señala Camerini, o.c. p. 816 que el sistema de caja de valores fue creado por la Ley N° 20.643, y originariamente lo integraban la Bolsa de Comercio de Buenos Aires, el Mercado de Valores de Buenos Aires y los mercados de valores del interior, quienes constituyeron Caja de Valores S.A.

Caja de Valores es un sistema de custodia y depósito de títulos valores. Es un ente autorizado para recibir depósitos colectivos de títulos públicos y privados. El depositante es la persona autorizada a efectuar el depósito colectivo, a cuenta propia o por cuenta ajena. El Comitente es el propietario de los títulos valores depositados en Caja de Valores. El depositante y Caja de Valores celebran un contrato de depósito regular. La Ley N° 26.831 creó el registro de Agentes de Depósito Colectivo, donde está inscripto CVSA. CVSA recibe depósito colectivo de títulos valores a la orden de los depositantes y a nombre de los comitentes, aunque una misma persona puede ser depositante y comitente. El depósito colectivo establece entre los comitentes una copropiedad indivisa sobre todos los títulos de la misma especie, clase y emisor depositados en CVSA. Para determinar la cuota parte que corresponde a cada copropietario, debe tenerse en cuenta el valor nominal de los títulos depositados. El depósito no transfiere a CVSA la propiedad ni el uso de los títulos depositados. CVSA abre una cuenta a nombre de cada depositante, que se subdivide en cuantos comitentes se denuncien y también en función de la especie, clase y emisor de títulos

depositados. CVSA asume responsabilidad por casos de fuerza mayor o caso fortuito.

[1958]

Para un estudio casuístico de cómo tales abusos se manifestaron, véase, del autor *Reflexiones sobre derivados sintéticos: la postura de la SEC en el caso Goldman Sachs*”, Eldial.com, Supl. Dcho. Empresario, Junio 2010.

[1959]

Confr. Fulvio Corsi, Hykel Hosni y Stefano Marmi, *Risk allocation: the double face of financial derivatives*, disponible al 15/05/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1844288.

[1960]

Confr. discurso de Charlie McCreevy, European Commissioner for Internal Market and Services

Derivatives and Risk Allocation, del 24 de Septiembre de 2009, disponible al 15/05/2020 en

https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_410.

[1961]

Ampliar en *Guía de negociación sobre Contratos de Futuros sobre Soja Chicago*, disponible al 15/05/2020 en

[https://www.rofex.com.ar/upload/reglamentos/CONTRATOS%20DE%20FUTUROS%](https://www.rofex.com.ar/upload/reglamentos/CONTRATOS%20DE%20FUTUROS%20)

[1962]

Ampliar en la obra de Rocío Carreras, *Contratos derivados*, publicado en Revista Argentina de Derecho Empresario, Número 9, 20/04/2011, disponible al 15/05/2020 en <https://ar.ijeditores.com/articulos.php?idarticulo=42156&print=2>

[1963]

Para un análisis profundo de esta operatoria contractual, véase, del autor *Reflexiones sobre derivados sintéticos: la postura de la SEC en el caso Goldman Sachs*”, Eldial.com, Supl. Dcho. Empresario, Junio 2010.

[1964]

Confr. <https://www.iprofesional.com/economia/270494-banco-central-bonos-deuda-Seguros-anti-default-y-una-mala-noticia-para-el-Gobierno-para-inversores-Argentina-es-mas-riesgosa-que-Grecia>, disponible al 15/05/2020.

[1965]

Puede ampliarse en la obra de Gregorio Álvarez Rubial, *El credit default swap como agente transformador del paradigma financiero internacional*, recuperado el 15/05/2020 en http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEE04-2013_EICDS_ParadigmaFinanciero_GAlvarez.pdf

[1966]

Ampliar en el interesante artículo de Adam Davidson, *How AIG fell apart*, recuperado el 15/05/2020 en <https://www.reuters.com/article/us-how-aig-fell-apart-idUSMAR85972720080918>

[1967]

Confr. KPMG, *El mercado de derivados financieros en Argentina*, disponible al 15/05/2020 en <https://assets.kpmg/content/dam/kpmg/ar/pdf/kpmg-informe-especial-derivados-financieros-en-el-mercado-argentino-2018.pdf>

[1968] El Art. 188 de la Ley N° 27.440 define a los pases como contratos (i) sujetos a la ley y jurisdicción argentina o extranjera y celebrados mediante acuerdos marcos o individuales o bajo los términos y condiciones establecidos por el mercado en el que se concierten; (ii) en los cuales se acuerde de manera simultánea (a) *la venta o compra al contado de valores negociables y/o cualquier activo financiero* y (b) *la obligación de recompra o reventa a plazo*; (iii) que se pueden celebrar y/o negociar en mercados autorizados por la Comisión Nacional de Valores o fuera de los mismos; y (iv) que incluyen, a modo enunciativo, los contratos de recompra (denominados en idioma inglés "*repurchase agreements*" o REPOs).

[1969] Ampliar en <https://www.firstcfa.com/es/prensa/183-moni-mobile-i-se-lanza-el-primer-fideicomiso-100-digital> recuperado el 15/05/2020.

[1970] Ampliar en <https://www.allaria.com.ar/INFORMES/20190215/83D2A1F6-6654-48CC-BA49-D9F158F7AE8DFF%20MC%20III%20SUPLE.PDF>, disponible al 15/05/2020.

[1971] Véase *supra* en § 4.5.13.2.

[1972] Se sigue, en general, la exposición del autor en *Prueba de Impacto: Token Economics y Sustainable Finance*, publicado en Diario La Ley, 09/12/2019.

[1973] Confr. <https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/> disponible al 15/05/2020.

[1974] Confr. <https://www.sustainablefinance.ch/en/what-is-sustainable-finance-content---1--1055.html> disponible al 15/05/2020.

[1975] Confr. <https://www.unpri.org/download?ac=6297> disponible al 15/05/2020.

[1976] Confr. https://www.unepfi.org/fileadmin/documents/InvestorStatement_ClimateChange_sp.r disponible al 15/05/2020.

[1977] Confr. Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf> disponible al 13/11/2019, pág. 4.

[1978] Confr. <https://www.nytimes.com/2019/10/22/climate/new-york-lawsuit-exxon.html> disponible al 15/05/2020. En este caso, la parte actora -Procurador del Estado de Nueva York- demanda a la empresa líder mundial del sector de hidrocarburos sosteniendo que ocultó o mintió sobre el impacto ambiental de sus operaciones, al planificar financieramente sus operaciones con un costo de carbón más bajo que el real, lo que habría implicado una manipulación fraudulenta en el

precio de la acción. El daño causado a los inversores se situaría entre 0.5 y 1.5 Billones de Dólares. El Estado de Massachusetts ha iniciado una demanda similar a la de New York. El caso representa la segunda demanda iniciada contra una compañía acusada de agravar el cambio climático con su modelo de negocios, que finalmente llega a juicio por no haber podido cerrar el caso con una transacción.

[1979]

Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf> disponible al 15/05/2020.

[1980]

Confr. Normas CNV TO 2013. Véase por ejemplo el Capítulo I, Art. 1, ap. a.1), al exigir que en la Memoria se informe acerca de la política de sustentabilidad, incluyendo, si tuvieran, los principales indicadores de desempeño de la emisora en la materia, o, en caso de no contar con tales políticas o indicadores, proporcionar una explicación de por qué los administradores de la emisora consideran que no son pertinentes para su negocio; el Capítulo VI, Anexo II, Prospecto para el panel PYME, al exigir que la emisora describa su política ambiental; el Capítulo IX, Anexo I, que describe el contenido del Prospecto de Emisión, apartado 5.c.2), y dispone que la emisora describa los aspectos ambientales como factor de riesgo de su modelo de negocios, identificando al regulador ambiental competente y detallando “*cualquier cuestión ambiental que pueda afectar la utilización de los activos de la empresa, incluyendo el estado de conservación para el caso de recursos naturales involucrados en el negocio.*” Finalmente, el Capítulo III, Anexo IV, dentro de los principios de gobierno corporativo, el sexto principio titulado “Mantener un vínculo directo y responsable con la comunidad” recomienda que las emisoras emitan anualmente un Balance de Responsabilidad Ambiental y Social verificado por un auditor externo independiente.

[1981]

Confr. en <https://www.boletinoficial.gob.ar/detalleAviso/primera/203933/20190322> disponible al 15/05/2020.

[1982]

Confr. <https://www.icmagroup.org/green-social-and-sustainability-bonds/green-bond-principles-gbp/> disponible al 15/05/2020.

[1983]

Confr. <https://www.icmagroup.org/green-social-and-sustainability-bonds/social-bond-principles-sbp/> disponible al 15/05/2020.

[1984]

Confr. <https://www.climatebonds.net/standard> disponible al 15/05/2020.

[1985]

Confr. Lineamientos para la Emisión de Bonos Verdes, Sociales y Sustentables, pág. 6.

[1986]

Refiere al riesgo de que los proyectos postulados no utilicen los fondos recaudados para las actividades declaradas, o que el proyecto no genere el impacto que

declaró al emitir los instrumentos de financiamiento. Confr. Lineamientos para la Emisión de Bonos Verdes, Sociales y Sustentables, pág. 10, nota 11.

[1987]

Confr. Lineamientos para la Emisión de Bonos Verdes, Sociales y Sustentables, pág. 14.

[1988]

Idem, pág. 15.

[1989]

Disponible en <https://www.icmagroup.org/green-social-and-sustainability-bonds/impact-reporting/> al 15/05/2020.

[1990]

Confr. [https://www.ey.com/Publication/vwLUAssets/EY-global-sustainability-taxes/\\$FILE/EY-global-sustainability-taxes.pdf](https://www.ey.com/Publication/vwLUAssets/EY-global-sustainability-taxes/$FILE/EY-global-sustainability-taxes.pdf) pág. 10, disponible al 15/05/2020.

[1991]

Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf> disponible al 15/05/2020, pág. 4.

[1992]

Ibid.

[1993]

Idem, p. 5. La utilización de smart contracts en la emisión y distribución de bonos elimina a los brokers y agentes de colocación, y también reduce el rol de los bancos como market makers e intermediarios con los inversores, reteniendo el proceso de KYC.

[1994]

Idem, p. 6. La utilización de smart contracts permite transferencias bi-direccionales de bienes y valor, sin necesidad de procesos separados de pago y liquidación, transfiriendo un activo digital -i.e, StableCoin- a cambio de un token (STOs) que representa el bono. Las fechas de pago y los importes de amortizaciones pactadas quedan automatizados, sin necesidad de intermediarios y sin riesgo de contraparte. Esto reduce drásticamente procesos humanos de 2 o 3 días, a transacciones inmediatas.

[1995]

Confr. <https://www.commbank.com.au/business/business-insights/project-bondi.html> disponible al 15/05/2020.

[1996]

Confr. <https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million> disponible al 15/05/2020.

[1997]

Confr. <https://www.worldbank.org/en/news/press-release/2019/08/16/world-bank-issues-second-tranche-of-blockchain-bond-via-bond-i> disponible al 15/05/2020.

[1998]

Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf>

[linked-bonds.pdf](#) disponible al 15/05/2020, pág. 9.

[1999]

Confr. <https://www.ledgerinsights.com/bbva-blockchain-structured-bond-mapfre/> disponible al 15/05/2020.

[2000]

Confr. <https://noticias.mapfre.com/mapfre-invierte-bono-verde/> disponible al 15/05/2020.

[2001]

Confr. <https://www.ledgerinsights.com/bbva-blockchain-structured-bond-mapfre/> disponible al 15/05/2020.

[2002]

Confr. <https://www.jpmorgan.com/global/news/digital-coin-payments> disponible al 15/05/2020.

[2003]

Confr. <https://www.fnality.org> disponible al 15/05/2020.

[2004]

Disponible en <https://www.icmagroup.org/assets/documents/Regulatory/Green-Bonds/June-2019/Handbook-Harmonized-Framework-for-Impact-Reporting-WEB-100619.pdf> al 15/05/2020.

[2005]

Idem, p. 10. Los indicadores clave de impacto ambiental son (i) la reducción o eliminación anual de gases de efecto invernadero (GEI) equivalente a toneladas de dióxido de carbono (CO₂); y (ii) generación anual de energía eléctrica medida en MWh/GWh.

[2006]

Idem, p. 11. Los indicadores clave de impacto ambiental son (i) el ahorro anual de energía eléctrica medida en MWh/GWh, y (ii) la reducción o eliminación anual de gases de efecto invernadero (GEI) equivalente a toneladas de dióxido de carbono (CO₂).

[2007]

Idem, p. 12. Algunos indicadores clave de impacto ambiental son (i) ahorros anuales de M³ de agua por re-utilización de agua, reducción de pérdidas, o menor consumo en actividades industriales, incluyendo el riego; o (ii) cantidad anual de agua residual tratada.

[2008]

Idem, p.15. Se utilizan indicadores de impacto tales como (i) cantidad anual de toneladas de residuos que son prevenidas, minimizadas, reusadas o recicladas, pudiendo en algunos casos informarse la posible captura de GEI por el proyecto; (ii) cantidad anual de energía medida en MWh/GWh generada en base a residuos no reciclables, pudiendo informarse la reducción de GEI generada por el proyecto equivalente a toneladas de dióxido de carbono (CO₂); (iii) cantidad de personas o porcentaje de población que se beneficia del servicio de tratamiento de residuos; o (iv) cantidad de personas involucradas en trabajos informales de reciclado incorporados a

procesos formales de reciclado.

[2009]

Idem, p. 20. Se utilizan métricas de impacto asociadas a transporte eléctrico, híbrido, público, trenes, no motorizados, multi-modal e infraestructura para vehículos de energía verde, tales como (i) a reducción o eliminación anual de gases de efecto invernadero (GEI) equivalente a toneladas de dióxido de carbono (CO₂); (ii) cantidad de pasajero/carga por kilómetro que utiliza el transporte sustentable; (iii) la reducción de contaminantes medido en partículas, sulfuros, monóxido de carbono y otros contaminantes; (iv) cantidad de vehículos verdes desplegados -bicicletas-; (v) reducción estimada de combustible; (vi) cantidad de kilómetros de vías férreas, biciesendas, carriles dedicados; (vii) reducción de ruidos en decibeles.

[2010]

Idem, p. 24. Algunos indicadores de impacto son: (i) porcentaje de energía renovable generada en el edificio; (ii) la reducción o eliminación anual de gases de efecto invernadero (GEI) equivalente a toneladas de dióxido de carbono (CO₂); (iii) cantidad anual de residuos reutilizados, reciclados o minimizados sobre el porcentaje total de residuos generados; (iv) porcentaje de superficie verde no afectada por el edificio; (v) M³ por año de agua de lluvia reutilizada; (vi) ahorro energético en KWh por instalación de fotocélulas; (vii) distancia en kilómetros hasta el transporte público.

[2011]

Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf> disponible al 15/05/2020, pág. 19.

[2012]

Confr. <https://www.undp.org/content/undp/en/home/blog/2019/adopting-a-cedar-tree-and-bringing-diaspora-money-home.html> disponible al 15/05/2020.

[2013]

Confr. <https://makerdao.com/es/> disponible al 15/05/2020.

[2014]

Posner, Richard, "The right of privacy", 12 Ga. L. Rev. 393 (1978).

[2015]

Confr. <https://techcrunch.com/2019/03/15/the-inevitability-of-tokenized-data/> disponible al 15/05/2020.

[2016]

Confr. <https://blogs.thomsonreuters.com/answerson/blockchain-compliance-efficiency/> disponible al 15/05/2020.

[2017]

Confr. <https://www.sustainablefinance.hsbc.com/-/media/gbm/reports/sustainable-financing/blockchain-gateway-for-sustainability-linked-bonds.pdf> disponible al 15/05/2020, pág. 24.

[2018]

Confr. Justin Cook, Richard Cohen y Jason Deniseko, *Initial Coin Offerings: a comparative overview of securities regulatory environments in the US, UK and Asia Pacific*, en Blockchain & Cryptocurrency Regulation, Global Legal Group, 2019,

disponible al 15/05/2020 en https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1_1.pdf, p. 34.

[2019] Disponible en <https://coincenter.org/files/2019-03/clayton-token-response.pdf> al 27/04/2020.

[2020] Disponibles, al 15/05/2020 en <https://www.sec.gov/files/dlt-framework.pdf>. Ampliar en Nikkita Mittal, *A closer look at the SEC's crypto token guidance*, disponible al 15/05/2020 en <https://theblockchainland.com/2019/04/15/closer-look-secs-crypto-token-guidelines/>.

[2021] Confr. Nikhilesh De, *SEC's crypto token framework falls short of clear and actionable guidance*, recuperado el 15/05/2020 en <https://www.coindesk.com/secs-crypto-token-framework-falls-short-of-clear-and-actionable-guidance>

[2022] Confr. en <https://www.sec.gov/files/dlt-framework.pdf>, nota 16, disponibles, al 15/05/2020.

[2023] Confr. en <https://www.sec.gov/files/dlt-framework.pdf>, pág. 10, disponibles al 15/05/2020

[2024] Confr. Brady Dale, *SEC issues first "no-action" letter clearing ICO to sell tokens in US*, disponible el 15/05/2020 en <https://www.coindesk.com/sec-issues-first-ever-no-action-letter-clearing-ico-to-sell-tokens-under-us-law>

[2025] Este requisito tiene su origen en el caso *Munchee, Inc.*

[2026] Confr. <https://www.sec.gov/litigation/admin/2020/33-10755.pdf>, recuperado el 15/05/2020.

[2027] Ibid.

[2028] Confr. <https://block.one/news/block-one-announces-settlement-with-us-securities-and-exchange-commission/> disponible al 15/05/2020.

[2029] Ampliar en Laura Shin, *Here's the man who created ICOs and this is the new token he's backing*, disponible al 15/05/2020 en <https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/#62cd4e9e1183>

[2030] SAFTs registrados en la SEC disponibles al 15/05/2020 <https://www.sec.gov/Archives/edgar/data/1729650/000095017218000060/0000950172-18-000060-index.htm>

[2031] Confr. <https://es.cointelegraph.com/news/telegram-refusing-to-tell-sec-how-it-spent-17-billion-of-ico-cash>, recuperada el 15/05/2020.

[2032] Ampliar en Anna Baydakova, *Telegram finally confirms it's behind TON blockchain*, recuperado el 15/05/2020 en <https://www.coindesk.com/telegram-finally-confirms-its-behind-ton-blockchain>. Ampliar también en <https://telegram.org/tos/wallet>, disponible al 15/05/2020. “Telegram’s blockchain is designed as a proof-of-stake protocol with the support of multiple “shardchains.” Validators, chosen from among those users who stake considerable amounts of tokens, will confirm the blocks. The TON blockchain will be compatible with ethereum-based software, according to TON Labs.” Confr. <https://www.coindesk.com/telegram-finally-releases-code-for-its-1-7-billion-ton-blockchain>, disponible al 15/05/2020.

[2033] Confr. <https://www.law360.com/articles/1231006/sec-seeks-full-telegram-bank-records-by-next-week> recuperado el 15/05/2020. Véase también <https://www.sec.gov/news/press-release/2019-212>. La SEC afirma que la venta global de *Gram* incluyó a 39 inversores de EE.UU, y que los Grams son un security sujeto a previa registraci3n.

[2034] Confr. Joshua Ashley Klayman, *Mutually assured disruption: the rise of the security token*, en *Blockchain & Cryptocurrency Regulation*, Global Legal Group, 2019, disponible al 15/05/2020 en https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1, p. 75.

[2035] Idem, p. 76

[2036] Confr. IOSCO, *Issues, risks and regulatory considerations relating to crypto-assets trading platforms*, disponible al 16/05/2020 en <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf>

[2037] Idem, p. 6.

[2038] Idem, p. 7.

[2039] Ibid.

[2040] Idem, p. 4.

[2041] Se sigue, en general, la exposici3n de Michelle Ann Gitlitz y Grant Buerstetta, *An introduction to virtual currency money transmission regulation*, en *Blockchain & Cryptocurrency Regulation*, Global Legal Group, 2019, disponible al 15/05/2020 en

https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.1

p. 132.

[2042]

Ibid.

[2043]

Idem, p. 133.

[2044]

Ibid.

[2045]

[2046]

Idem, p. 134.

[2047]

Ibid. “*User: a person who obtains virtual currency to purchase goods or services. In January 2014, this definition was expanded to also include **businesses that are strictly investing in convertible virtual currency for their own account and not for any other party.** Under the current Guidance, it would appear that institutions investing in virtual currencies such as co-mingled investment funds are considered users.*”

[2048]

Ibid. “*Exchanger: a person engaged **as a business** in the exchange of virtual currency for real currency, funds, or other virtual currency. Note that a person must be engaged in a business; thus, **trading simply for personal investment purposes does not qualify one as an exchanger.** In addition, one must accept and transmit virtual currency from one person to another or to another location, such as a brokerage service or trading platform. **Mere acceptance of virtual currency in exchange for providing a good or service does not make a person a money transmitter.***”

[2049]

Ibid. “***Administrator: a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.***”

[2050]

Idem, p. 135. “Application of FinCEN’s **Regulations to Virtual Currency Software Development and Certain Investment Activity**, FIN-2014-R002 (Jan. 30, 2014) (the “2014 Software and Investment Guidance”); Application of FinCEN’s **Regulations to Virtual Currency Mining Operations**, FIN-2014-R001 (Jan. 30, 2014) (the “2014 Mining Guidance”); and Request for Administrative Ruling on the Application of FinCEN’s **Regulations to a Virtual Currency Payment System**, FIN-2014-R012 (Oct. 27, 2014) (the “2014 Payment System Ruling”).”

[2051]

Ibid. “*Software developer: The production and distribution of virtual currency-related software, in and of itself, **are not money transmission services and the entity engaged in the activity is not a money transmitter, even if the purpose of the software***

is to facilitate the sale of virtual currency.”

[2052]

Ibid. “Miners play a vital role in allowing many decentralized blockchain-based virtual currency systems to operate properly. Mining is important because virtual currencies or tokens such as Bitcoin are initially acquired through mining; unlike paper money, decentralized virtual currencies do not have a central government to issue the currency. This provides a somewhat controlled way to distribute tokens and creates a real incentive for miners to enter the market. Miners also play another vital role; in the traditional banking system, banks maintain an accurate record of parties and details of each transaction; however, since there is no central regulator for decentralized virtual currencies, the miners assume this role. **Those who mine virtual currencies, whether by “earning,” “harvesting,” “creating,” or “manufacturing,” are all classified as users and not money transmitters.** Once the virtual currency is mined, a miner, depending on how he/she uses the convertible virtual currency and for whose benefit, may potentially become a money transmitter. Just because the miner acquired the tokens directly by mining them, rather than purchasing or being given them, his/her status as a user is unaffected. Miners may use their mined tokens or currencies to purchase goods, and until they engage in activities that would qualify them as a transmitter, they remain a user.”

[2053]

Ibid. “A convertible virtual currency that has a centralized repository is a centralized virtual currency (“CVC”). **The repository of a CVC is a money transmitter to the extent that it allows transfers of value between persons or from one location (i.e., a user’s account in New York) to another (i.e., that user’s account in California).** In addition, if the CVC repository accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the repository’s own convertible virtual currency, and then transmits that internally credited value to third parties at the user’s direction, **the CVC repository is a money transmitter.**”

[2054]

Ibid. “Decentralized virtual currencies: A decentralized virtual currency (“DVC”) is a virtual currency that has no central repository and no single person who has the ability to issue or redeem the virtual currency. Persons may obtain the virtual currency through their own computing or mining effort or by purchasing the currency. **A person who creates units of a DVC and uses it to purchase real or virtual goods and services is a “user” of the convertible virtual currency and is not subject to regulation as a money transmitter. By contrast, a person who creates units of a DVC, and sells those units to another person for real currency or its equivalent and is engaged in that transfer as a business, is a money transmitter to the extent that he/she is transferring it from one person or location to another person or location.** A person who accepts and transmits real currency to one person in exchange for a DVC, but is arguably engaged in the business of providing goods

and services, may have a valid argument that he/she is not a money transmitter. The exact scope of the regulation in this context is currently unclear.”

[2055]

Idem, p. 136. “Wallets: **are secure virtual currency storage systems used to hold and potentially send or receive virtual currency. Most virtual currencies have official or suggested wallets and the use of a wallet is necessary.** The wallet contains a public and private key for each virtual currency address. The private key is a secret number that allows the virtual currency to be spent. The public key is used to ensure the wallet holder is the owner of the wallet address and can receive funds. **The public key is mathematically derived from the private key. The status of a wallet as a money transmitter is primarily determined by whether or not the wallet company has custody of the private keys for the virtual currency.** Custodial wallets: **Custodial wallet companies are likely money transmitters.** They typically accept virtual currencies for users and transmit them when the currencies need to be moved. The custodial wallet is in full control of the transaction and the user could not facilitate the transaction without the participation and action of the wallet provider. Examples of custodial wallet companies include Bitfinex, Bitthumb and Coinbase.

Non-custodial wallets: **Non-custodial wallet companies are likely not money transmitters.** These wallets never accept or transmit virtual currencies; **they are a software tool.** The user facilitates the transaction and neither the wallet nor the keys are ever in the possession of the non-custodial wallet company. This entity can be thought of as merely a developer of software used to aid the customer in facilitating his/her own transactions. Examples of non-custodial wallet companies include Jaxx, BitGo and Mycellium.”

[2056]

Ibid. “**Custodial exchanges:** are virtual currency exchange platforms on which users are able to buy and sell virtual currencies. What distinguishes this type of exchange as custodial is the fact that the exchange is in control of a user’s funds, or in other words, **the exchange is the custodian of the private keys for the virtual currencies or tokens.** Examples of these types of exchanges include Coinbase, GDAX, Kraken, and Bitfinance. **Custodial exchanges are money transmitters** because they are both buying and selling, and accepting and transmitting virtual currencies. Non-custodial exchanges: are virtual currency exchange platforms on which users are able to purchase and sell virtual currencies. What makes the non-custodial exchange different from the custodial exchange is that **the exchange never takes possession of the user’s virtual currency or private keys.** Examples include Shape Shift and Evercoin. **Non-custodial exchanges are likely not money transmitters.** They are merely a source to help connect potential buyers with potential sellers, similar to a message or classifieds board like Craigslist. Because they are never in possession of the currency or private keys, they are never accepting or transmitting, and they are not buying or selling.”

[2057] Ibid. “Token developers: are the **individuals who create a token platform and the virtual currency**. A token developer who either gives away his/her tokens or allows mining is simply distributing his/her software and, absent other facts, **is not a money transmitter**. These token developers never accept and transmit tokens, but rather are simply developing and distributing the software in order to allow other users to operate peer-to-peer. Whether token developers are subject to regulation depends on the business they are engaged in and whether they are a DVC or CVC (...) A token developer who sells virtual currency or tokens to users, rather than giving them away or allowing users to mine currency, is more complex. **A miner who sells the currency he has mined and a developer who sells currency he has created should be treated the same**. At the outset, the Guidance does not address these scenarios and there is not yet any case law in the area. However, in FinCEN’s first civil enforcement action against a virtual currency exchanger, Ripple Labs Inc., FinCEN alleged that Ripple Labs’ currency, XRP, made the developer an exchanger subject to BSA regulation.”

[2058] Confr. FinCEN, *New FinCEN Guidance Affirms Its Longstanding Regulatory Framework for Virtual Currencies and a New FinCEN Advisory Warns of Threats Posed by Virtual Currency Misuse*, disponible el 16/05/2020 en <https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual>

[2059] Ibid, p. 27.

[2060] Ibid.

[2061] Confr. Michelle Ann Gitlitz y Grant Buerstetta, *An introduction to virtual currency money transmission regulation...o.c.*, p. 137.

[2062] Confr. <https://www.coindesk.com/stonewalled-by-finra-up-to-40-crypto-securities-wait-in-limbo-for-launch> recuperado el 16/05/2020.

[2063] Confr. FINRA, *Distributed ledger technology: implications of blockchain for the Securities industry*, disponible al 16/05/2020 en https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

[2064] Confr. la Asociación Japonesa de Casas de Cambio de Monedas Virtuales (JVCEA, en inglés), véase <https://medium.com/@newscnofficial/the-japan-virtual-currency-exchange-association-jvcea-japans-official-self-regulatory-body-341d6e2817e8>, recuperado el 28/04/2020.

[2065] Confr. <https://news.bitcoin.com/japan-cryptocurrency-industry-self-regulation/>, recuperado el 27/04/2020

[2066] La demanda de la CFTC está disponible, al 15/06/2020 en <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/docu>

[2067] Idem, p. 2.

[2068] Confr. https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcfctc_prim disponibles al 16/05/2020.

[2069] Ibid.

[2070] Ibid.

[2071] Confr. <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>, recuperado el 16/05/2020.

[2072] Confr. https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf recuperado el 16/05/2020.

[2073] Idem, p. 20.

[2074] Confr. Sheppard Mullin, *Smart contract developers – beware and lawyer up!*, disponible al 17/05/2020 en <https://www.lexology.com/library/detail.aspx?g=62c4eafb-376e-48df-adf2-0f78303c9dae>

[2075] Confr. Malcolm Falzon y Alexia Valenzia, *Malta*, en Blockchain & Cryptocurrency Regulation, Global Legal Group, 2019, disponible al 15/05/2020 en https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.1 p. 378.

[2076] Idem, p. 379.

[2077] Confr. <https://news.bitcoin.com/malta-blockchain-island-deferred-licensing/> recuperado el 16/05/2020.

[2078] Confr. <https://www.mfsa.mt/news-item/warning-to-the-public-regarding-unlicensed-vfa-companies/> recuperado el 16/05/2020.

[2079] Ibid.

[2080] Confr. <https://www.gamblingnews.com/news/malta-crypto-gambling-initiative-progresses-to-phase-2/> recuperado el 16/05/2020.

[2081] Véase www.augur.net y <https://medium.com/crypto-nyc/augur-explained-63455a0f6b37> recuperado el 17/05/2020.

[2082] Confr. María Florencia Moren, *El impuesto digital en el mundo*, Centro de Estudios en Administración Tributaria, UBA, disponible al 16/05/2020 en <http://www.economicas.uba.ar/wp-content/uploads/2019/02/LA-ECONOMIA-DIGITAL-EN-EL-MUNDO-FINAL.pdf>, p. 4.

[2083] Idem, p. 2.

[2084] Confr. <https://www.rte.ie/news/business/2019/1009/1082056-oecd-digital-tax-proposals/> disponible al 16/05/2020.

[2085] Idem, p. 9.

[2086] Idem, p. 12.

[2087] Idem, p. 14.

[2088] Confr. <https://www.oecd.org/tax/beps/inclusive-framework-on-beps-progress-report-july-2018-may-2019.pdf> recuperado el 15/05/2020.

[2089] Confr. https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en, recuperado el 15/05/2020.

[2090] Se sigue, en general, la exposición de Alexandra Sims, Kanchana Kariyawasam y David Mayes, *Regulating cryptocurrencies in New Zealand*, The Law Foundation New Zealand, disponible al 16/05/2020 en https://www.interest.co.nz/sites/default/files/embedded_images/Sims%20et%20al%20I

[2091] Idem, p. 82.

[2092] Confr. <https://www.ato.gov.au/Business/GST/In-detail/Your-industry/Financial-services-and-insurance/GST-and-digital-currency/> recuperado el 16/05/2020.

[2093] Confr. <https://es.cointelegraph.com/news/tether-launches-gold-backed-stablecoin-and-begins-trading-on-bitfinex> recuperado el 16/05/2020. Tether ofrece una *stablecoin* respaldada con oro, XAUT, que representa la propiedad de una onza troy de oro que se encuentra en una bóveda suiza controlada por la empresa.

[2094] Confr. <https://www.ato.gov.au/Business/GST/In-detail/Your-industry/Financial-services-and-insurance/GST-and-digital-currency/> recuperado el 15/05/2020.

[2095] Confr. Alexandra Sims, Kanchana Kariyawasam y David Mayes, *Regulating cryptocurrencies in New Zealand...o.c.*, p. 87.

[2096] Confr. <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies> recuperado el 17/05/2020.

[2097] Ibid.

[2098] Confr. <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses>, disponible al 16/05/2020.

[2099] Confr. Alexandra Sims, Kanchana Kariyawasam y David Mayes, *Regulating cryptocurrencies in New Zeland...o.c.*, p. 90.

[2100] Confr. <https://www.mondaq.com/canada/sales-taxes-vat-gst/287988/bitcoins-more-guidance-from-the-cra> recuperado el 16/05/2020.

[2101] Confr. <https://www.loc.gov/law/foreign-news/article/estonia-rules-on-taxation-of-bitcoin/> disponible al 16/05/2020.

[2102] Confr. <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/japan>, disponible al 16/05/2020.

[2103] Confr. <https://www.irs.gov/newsroom/irs-reminds-taxpayers-to-report-virtual-currency-transactions> recuperado el 16/05/2020.

[2104] Ibid.

[2105] Confr. Alexandra Sims, Kanchana Kariyawasam y David Mayes, *Regulating cryptocurrencies in New Zeland...o.c.*, p. 97.

[2106] Confr. <https://www.forbes.com/sites/kellyphillipserb/2019/09/19/portugal-tax-authorities-clarify-that-buying-or-selling-cryptocurrency-is-tax-free/#15e943a677e3> disponible al 16/05/2020.

[2107] Confr. <https://www.colombiafintech.co/novedades/como-declarar-sus-bitcoins-a-la-hora-de-pagar-impuestos> recuperado el 16/05/2020.

[2108] Idem, p. 52.

[2109] Confr. Julián Zambrano Sánchez y otros, *Aspectos tributarios de las transacciones en criptomonedas: el caso de los bitcoins*, publicado en la Revista del Instituto Colombiano de Derecho Tributario, Num. 80, Año 56, y recuperado el 16/05/2020 en https://revistaicdt.icdt.co/wp-content/Revista%2080/PUB_ICDT_AR_ZAMBRANO%20Julian_YEPES%20Santiago p. 46.

[2110] Idem, p. 47.

[2111] Idem, p. 58.

[2112] Idem, p. 60.

[2113] Idem, p. 62.

[2114] Idem, p. 64.

[2115] Confr. Francisco Ossandón Cerda, *Tributación de las criptomonedas en Chile: desafíos regulatorios actuales*, Centro de Estudios Tributarios de la Universidad de Chile, recuperado el 16/05/2020 en https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwj_9-H-o7vpAhUOHrkGHQFFBqMQFjABegQIAxAB&url=https%3A%2F%2Frevistas.uchile.

[2116] Idem, p. 113.

[2117] Idem, p. 122.

[2118] Idem, p. 128.

[2119] Idem, p. 131.

[2120] Se sigue en este apartado, en general, la opinión de Martina Caunedo, en *Una abogada experta en criptomonedas explica qué impuestos hay que pagar en la Argentina*, disponible al 16/05/2020 en <https://www.infobae.com/cripto247/altcoins/2018/07/20/una-abogada-experta-en-criptomonedas-explica-que-impuestos-hay-que-pagar-en-la-argentina/>.

[2121] Ibid.

[2122] Confr. Oscar Fernández, *Impuesto a las ganancias. Reforma Ley 27.430. Sociedades*, 27/03/2019, Federación Argentina de Concejos Profesionales de Ciencias Económicas, p. 34, disponible al 16/05/2020 en <https://www.cpba.com.ar/ipit/ContenidosMinimos/CO60002165.pdf>

[2123] Idem, p. 21.

[2124] Confr. Martina Caunedo, en *Una abogada experta en criptomonedas explica qué impuestos hay que pagar en la Argentina*, disponible al 16/05/2020 en <https://www.infobae.com/cripto247/altcoins/2018/07/20/una-abogada-experta-en-criptomonedas-explica-que-impuestos-hay-que-pagar-en-la-argentina/>.

[2125] Ibid.

[2126] Ibid.

[2127] Ibid.

[2128] Disponible al 16/05/2020 en <http://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verUnicoDocumentoLink.html?idAnalisis=739804&cache=1589736743996>

[2129] Idem, considerando 4°.

[2130] Idem, considerando 7°.

[2131] Ibid.

[2132] Ibid.

[2133] Confr. Roger Brownsword, *Regulatory fitness: Fintech, Funny Money and Smart Contracts*, publicado en *European Business Organization Law Review*, 2019, número 20, p. 11. Ejemplifica Brownsword a los “coherentes” en estos términos: “*When they are called on to respond to new technological developments, **coherentists tend to try to classify the new phenomena within existing legal categories. For example, a nice coherentist question might be whether, with humans out of the transactional loop, automated and autonomous performance systems could be treated relative to recognised legal concepts and categories (such as the limited liability company) as having their own legal personality. Similarly, when the technologies that support e-commerce appeared, the coherentist response was to try to fit the legal template for off-line contracts to the emerging world of on-line transactions.***”. Ejemplifica el enfoque de regulación instrumental en este modo: “*Unlike a coherentist conversation, a regulatory-instrumentalist conversation will not focus on the application of the law of contract to smart contracts. Rather, the conversation will seek to **identify the potential benefits and risks of committing transactions (or parts of transactions) to a blockchain and it will then strive to find an acceptable balance between management of the risks and not stifling enterprise. The challenge is to find the regulatory sweet spot, neither over-regulating (and stifling innovation) nor under-regulating and exposing parties to unacceptable risks.***” Los resaltados son míos.

[2134] En este sentido, la Asociación de Bancos Argentinos ha afirmado que existen asimetrías regulatorias e impositivas que favorecen a las Fintech y perjudican a los bancos. Confr. <https://gvainfo.com/2019/06/12/adeba-advirtio-que-existen-asimetrias-regulatorias-con-las-fintech/> disponible al 8/05/2020.

[2135] Confr. Recuperado el 8/05/2020 <https://www.cronista.com/finanzasmercados/Argentina-es-el-pais-de-la-region-que->

[mas-transformo-su-banca-digital-20180801-0082.html](https://www.ipsos.com/ma/mas-transformo-su-banca-digital-20180801-0082.html)

[2136]

Confr., *El BCRA amplía el margen de los bancos para que financien el pago de sueldos de estatales*, recuperado el 8/05/2020 de <https://www.iprofesional.com/inflacion/306503-prestamos-publico-banco-central-El-BCRA-amplia-el-margen-para-que-bancos-financien-sueldos-estatales>

[2137]

Confr. Dictamen versión no confidencial, en Expte. C.1613, https://www.argentina.gob.ar/sites/default/files/dictamen_prisma.pdf recuperado el 8/05/2020. Algunos puntos salientes del dictamen elaborado por la CNDC son que se investigó a 14 bancos y que incluso MercadoLibre S.R.L fue una de las entidades denunciadas. La conducta investigada, que combinó cartelización y abuso de posición dominante, fue tan patética y obscena que los Bancos investigados terminaron ofreciendo una desinversión para archivar la causa y evitar una multa multimillonaria, siendo la primera vez en la historia argentina que una investigación por conducta anticompetitiva termina con una desinversión. El compromiso de desinversión está disponible al 8/05/2020 en https://www.argentina.gob.ar/sites/default/files/compromiso_prisma.pdf. Penoso, por donde se lo mire...

[2138]

Confr. <https://www.economista.com.ar/2019-06-mas-del-50-de-los-adultos-esta-afuera-del-sistema-financiero/> disponible al 15/05/2020.

[2139]

Confr. <https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html> recuperado el 16/05/2020.

[2140]

Véase <https://www.powerledger.io>

[2141]

Véase <https://www.wepower.com>

[2142]

Véase <https://enerchain.ponton.de>

[2143]

Para un estudio profundizado sobre la aplicación de smart contracts a los mercados minoristas de energía con generación distribuida, véase la interesante obra de Hu, W., Hu, Y.W., Yao, W.H., Lu, W.Q., Li, H.H., y Lv, Z.W., *A blockchain-based smart contract trading mechanism for energy power supply and demand network*, en *Advances in Production Engineering & Management*, Vol. 14, Núm. 3, Septiembre de 2019, p. 284.

[2144]

Véase <https://gridplus.io/energy>

[2145]

Véase <https://www.brooklyn.energy>

[2146]

Véase <https://www.greeneum.net>

[2147] Véase <https://gridsingularity.com>

[2148] Confr. <https://medium.com/@GridSingularity/deploying-local-electricity-markets-to-optimise-pv-integration-a-study-of-three-lem-scenarios-in-cf125b26f4dc> disponible al 16/05/2020.

[2149] Disponible al 16/05/2020 en http://www3.weforum.org/docs/WEF_Windows_of_Opportunity.pdf

[2150] Idem, p. 10.

[2151] Idem, p. 13.

[2152] Véase <https://www.tradelens.com>

[2153] Confr. <https://www.tradelens.com/press-releases/indonesia-shipping-supply-chains-to-join-ibm-and-maersks-tradelens-to-strengthen-logistic-services> disponible al 16/05/2020.

[2154] Confr. <https://medium.com/the-capital/blockchain-for-letter-of-credit-319436c63bc1> disponible al 16/05/2020.

[2155] Ibid.

[2156] Confr. <https://www.ledgerinsights.com/letter-of-credit-blockchain-contour-hsbc-ing/> disponible al 17/05/2020.

[2157] Ibid.

[2158] Confr. <https://www.globaltrademag.com/blockchain-smart-contracts-supply-chains/> disponible al 16/05/2020.

[2159] Véase <https://www.vechain.com>

[2160] Ampliar en <https://bbs.vechainworld.io/topic/254/democratizing-the-automobile-industry-with-blockchain-technology-the-new-vechain-and-bmw-partnership-explained> y en <https://digitalasset.live/2019/05/04/bmw-goes-blockchain-with-vechain/>, disponibles al 16/05/2020.

[2161] Confr. <https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/blockchain-50/#1c12051d7553> recuperado el 16/05/2020.

[2162] Confr. <https://www.daimler.com/sustainability/resources/blockchain-pilot-project-supply-chain.html> disponible al 16/05/2020.

[2163] Confr. <https://dailyhodl.com/2020/03/18/worlds-second-largest-automaker-reveals-plan-to-accelerate-use-of-blockchain-technology/> recuperado el 27/05/2020.

[2164] Confr. <http://www.jcnnewswire.com/pressrelease/57825/3/> disponible al 17/05/2020.

[2165] Confr. <https://www.godirecttrade.com/blockchain>

[2166] Confr. <https://www.forbes.com/sites/michaeldelcastillo/2020/02/19/blockchain-50/#1c12051d7553> recuperado el 16/05/2020.

[2167] Confr. <https://www.reuters.com/article/us-banks-blockchain-exclusive/exclusive-banks-to-invest-around-50-million-in-digital-cash-settlement-project-sources-idUSKCN1SM2U0> recuperado el 16/05/2020.

[2168] Véase <https://www.fnality.org/about-fnality>

[2169] Confr. <https://www.fnality.org/what-we-do> recuperado el 17/05/2020.

[2170] Confr. <https://cryptonews.com/exclusives/financial-giants-backed-fnality-to-launch-first-usc-token-th-5768.htm> disponible al 16/05/2020.

[2171] Confr. <https://es.cointelegraph.com/news/jpmorgans-blockchain-products-explained-by-ex-jpm-tech-leads> recuperado el 16/05/2020.

[2172] Ibid.

[2173] Confr. <https://www.investopedia.com/jpmorgan-to-launch-jpm-coin-4587182> recuperado el 17/05/2020.

[2174] Ibid.

[2175] Ampliar en <https://cointelegraph.com/news/us-bitcoin-derivatives-market-highlights-of-2019> disponible al 16/05/2020.

[2176] Confr. <https://fortune.com/2020/02/05/bakkt-rewards-points-bitcoin-cash-wallet/> recuperado el 17/05/2020.

[2177] Confr. <https://www.bakkt.com/bakkt-markets> recuperado el 16/05/2020.

[2178] Véase <http://www.synapsloans.com>

[2179] Confr. <http://www.synapsloans.com/press-releases/> disponible al 16/05/2020.

[2180] Véase <https://www.capgemini.com/service/syndicated-loans/>

- [2181] Confr. <https://www.marcopolo.finance>
- [2182] Confr. <https://www.marcopolo.finance/about/>
- [2183] Confr. <https://www.bbva.com/en/bbva-signs-world-first-blockchain-based-syndicated-loan-arrangement-with-red-electrica-corporacion/> recuperado el 17/05/2020.
- [2184] Confr. <https://www.bbva.com/en/the-banker-recognizes-bbvas-blockchain-corporate-lending-platform/> recuperado el 17/05/2020.
- [2185] Confr. <https://www.bbva.com/en/the-banker-recognizes-bbvas-blockchain-corporate-lending-platform/> recuperado el 17/05/2020.
- [2186] Confr. <https://www.bbva.com/en/bbva-and-madrids-government-close-the-first-blockchain-powered-sustainable-schuldschein-loan/> recuperado el 17/05/2020.
- [2187] Confr. <https://www.whitecase.com/publications/alert/schuldscheine-global-alternative-product-future>, recuperado el 17/05/2020.
- [2188] Confr. <https://www.ledgerinsights.com/blockchain-loan-schuldschein-bbva-madrid/> recuperado el 17/05/2020.
- [2189] Confr. <https://www.wavegp.com>
- [2190] Confr. <https://www.prnewswire.com/news-releases/wave-financial-launches-world-first-bitcoin-yield-fund-wave-btc-income--growth-digital-fund-300921154.html> recuperado el 17/05/2020.
- [2191] Confr. <https://www.wavegp.com/funds/wave-kentucky-whiskey> recuperado el 17/05/2020.
- [2192] Confr. <https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html#> disponible al 17/05/2020.
- [2193] Idem, p. 6.
- [2194] Idem, p. 12.
- [2195] Idem, p. 14.
- [2196] Véase <https://atlant.io>
- [2197] Véase <https://midasium.herokuapp.com>
- [2198] Confr. <https://midasium.herokuapp.com/about> recuperado el 17/05/2020.

- [2199] Confr. <https://consensys.net/blockchain-use-cases/real-estate/#loans> recuperado el 17/05/2020.
- [2200] Confr. <https://www.ledgerinsights.com/fitch-blockchain-securitization-china-leads/> recuperado el 17/05/2020.
- [2201] Véase <https://www.figure.com/blockchain/>
- [2202] Confr. <https://www.mpamag.com/news/figure-closes-first-ever-mortgage-securitization-on-a-blockchain-216875.aspx> recuperado el 17/05/2020.
- [2203] Ibid.
- [2204] Confr. <https://openledger.info/insights/blockchain-healthcare-use-cases/> recuperado el 17/05/2020.
- [2205] Véase <https://medrec.media.mit.edu>
- [2206] Confr. <https://medrec.media.mit.edu>
- [2207] Véase <https://medicalchain.com/en/partnership/> recuperado el 17/05/2020.
- [2208] Véase <https://phros.io/#home>
- [2209] Confr. <https://medium.com/@farmatrust/farmatrust-progress-report-dec-2018-4282442de07b> disponible al 17/05/2020.
- [2210] Confr. <https://blog.ambrosus.com/the-globalisation-of-pharma-a94b9533a80> disponible al 17/05/2020.
- [2211] Confr. <https://www.outsourcing-pharma.com/Article/2019/02/14/Boehringer-Ingelheim-and-IBM-bring-blockchain-to-clinical-trials> recuperado el 17/05/2020.
- [2212] Confr. <https://openledger.info/insights/blockchain-healthcare-use-cases/> recuperado el 17/05/2020.
- [2213] Ibid.
- [2214] Confr. <https://www.forbes.com/sites/amazonwebservices/2019/12/12/nestles-chain-of-origin-coffee-brings-supply-chain-transparency-with-amazon-managed-blockchain/#7ca3f0e7193b> recuperado el 17/05/2020.
- [2215] Confr. <https://agfundernews.com/cargill-and-agrocorp-complete-groundbreaking-12m-intercontinental-wheat-trade-using-hyperledger-fabric.html> recuperado el 17/05/2020.

- [2216] Ibid.
- [2217] Confr. <https://www.forbes.com/sites/biserdimitrov/2019/12/05/how-walmart-and-others-are-riding-a-blockchain-wave-to-supply-chain-paradise/#3a31bc277918> recuperado el 17/05/2020.
- [2218] Confr. <https://www.ibm.com/blockchain/solutions/food-trust> recuperado el 17/05/2020.
- [2219] Confr. <https://www.forbes.com/sites/biserdimitrov/2019/12/05/how-walmart-and-others-are-riding-a-blockchain-wave-to-supply-chain-paradise/#3a31bc277918> recuperado el 17/05/2020.
- [2220] Véase <https://www.everledger.io>
- [2221] Confr. <https://www.businessinsider.com.au/everledger-ledger-diamonds-blockchain-tech-theft-fraud-2015-8> recuperado el 17/05/2020.
- [2222] Confr. <https://b3i.tech/home.html>
- [2223] Confr. http://mercadoasegurador.com.ar/Newsletter_publico/edicion_11_2018/undecimo%20 recuperado el 17/05/2020.
- [2224] Confr. <https://www.insurancejournal.com/news/international/2020/02/14/558428.htm> disponible al 17/05/2020.
- [2225] Confr. <https://www.acord.org/ACORD-about/ACORD-About>
- [2226] Confr. <https://www.ledgerinsights.com/acord-insurers-blockchain/> recuperado el 17/05/2020.
- [2227] Confr. http://mercadoasegurador.com.ar/Newsletter_publico/edicion_11_2018/undecimo%20 recuperado el 17/05/2020.
- [2228] Confr. <https://www.ledgerinsights.com/marsh-proof-of-insurance-blockchain/> recuperado el 27/05/2020.
- [2229] Ibid.
- [2230] Véase <https://etherisc.com>
- [2231] Confr. <https://builtin.com/blockchain/blockchain-insurance-companies>

recuperado el 17/05/2020.

[2232] Véase <https://etherisc.com/faq>

[2233] Véase <https://guardtime.com/scm>

[2234] Confr. <https://builtin.com/blockchain/blockchain-insurance-companies>
recuperado el 17/05/2020.

[2235] Véase <https://www.fidentiax.com>

[2236] Confr. <https://builtin.com/blockchain/blockchain-insurance-companies>
recuperado el 17/05/2020.

[2237] Véase <https://www.axa.co.uk/manage-your-policy/>

[2238] Confr. <https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy>
recuperado el 17/05/2020.

[2239] Ibid.

[2240] La resolución está disponible, al 17/05/2020 en
<https://www.boletinoficial.gob.ar/detalleAviso/primera/213806/20190821>

[2241] Confr. <https://www.argentina.gob.ar/superintendencia-de-seguros/ mesa-de-innovacion-en-seguros-e-insurtechs> disponible al 17/05/2020.

[2242] La resolución está disponible, al 17/05/2020 en
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/307742/norma.htm>

[2243] Confr. <https://cognate.com/technical/>

[2244] Confr. <https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/> recuperado el 17/05/2020.

[2245] Confr. <https://www.searchenginewatch.com/2020/02/26/how-blockchain-will-dominate-the-digital-advertising-industry-in-2020/> recuperado el 17/05/2020.

[2246] Ibid.

[2247] Confr. <https://tech.economictimes.indiatimes.com/news/internet/facebook-to-pay-40m-for-inflating-data-on-video-ads/71492699> disponible al 17/05/2020.

[2248] Confr. <https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/antitrust/facebook-abuses-market-power-with-data-collection-from->

[multiple-sites-germany-says](#) disponible al 17/05/2020.

[2249]

Confr. <https://coreblog.lexxion.eu/doj-google-investigation/> y <https://www.digitaltrends.com/social-media/ftc-might-finally-do-something-about-facebooks-social-media-monopoly/> recuperadas el 17/05/2020.

[2250]

Confr. <https://www.cnbc.com/2019/10/22/47-attorneys-general-are-investigating-facebook-for-antitrust-violations.html> recuperado el 17/05/2020.

[2251]

Confr. <https://www.searchenginewatch.com/2020/02/26/how-blockchain-will-dominate-the-digital-advertising-industry-in-2020/> recuperado el 16/05/2020.

[2252]

Ibid.

[2253]

Confr. <http://certificates.media.mit.edu>

[2254]

Confr. <https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-ae03622426f> recuperado el 17/05/2020.

[2255]

Ibid.

[2256]

Confr. <https://www.dacs.org.uk/latest-news/report-art-market-powered-by-blockchain?category=For+Artists&title=N> recuperado el 17/05/2020. Véase el interesante estudio titulado *The Art Market 2.0: blockchain and financialisation in Visual Arts*, disponible al 17/05/2020 en <https://www.dacs.org.uk/DACSO/media/DACSDocs/Press%20releases/The-Art-Market-2-0-Blockchain-and-Financialisation-in-Visual-Arts-2018.pdf>.

[2257]

Confr. <https://medium.com/artory/artory-collaborates-with-christies-on-an-industry-first-registration-of-major-art-collection-5228ed94a567> recuperado el 17/05/2020.

[2258]

Véase <https://www.artory.com>

[2259]

Véase <https://www.liveauctioneers.com/pages/biddable/>

[2260]

Confr. <https://panoramacrypto.com/blockchain-boosts-art-market-results/> recuperado el 17/05/2020.

[2261]

Confr. <https://www.maecenas.co>

[2262]

Confr. <https://panoramacrypto.com/blockchain-boosts-art-market-results/> recuperado el 17/05/2020.

[2263]

Confr. <https://www.gartner.com/smarterwithgartner/5-ways-blockchain-will-affect-hr/> recuperado el 17/05/2020.

[2264] Confr. <https://empresas.blogthinkbig.com/blockchain-en-formacion-corporativa-proyecto-karma-de-telefonica/> recuperado el 17/05/2020. Otros casos de blockchain aplicado a la gestión del personal pueden verse en <https://www.hrtechnologist.com/articles/digital-transformation/top-blockchain-hr-startups/> y en <https://voice-on-growth.mercer.com/en/articles/innovation/blockchain-for-human-resources.html> recuperados el 17/05/2020.

[2265] Confr. <https://www.forbes.com/sites/rogerhuang/2019/01/27/how-blockchain-can-help-with-the-refugee-crisis/#672cabea6562> recuperado el 17/05/2020.

[2266] Ibid.

[2267] Confr. <https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/04/fs.pdf> disponible el 17/05/2020.

[2268] Confr. <https://cointelegraph.com/news/finland-solves-refugee-identity-with-blockchain-debit-cards> recuperado el 17/05/2020.

[2269] Confr. <https://www.fastcompany.com/40500978/this-new-blockchain-project-gives-homeless-new-yorkers-a-digital-identity> recuperado el 17/05/2020.

[2270] Confr. <https://www.forbes.com/sites/darrynpollock/2020/02/27/blockchain-for-good-how-the-united-nations-is-looking-to-leverage-technology/#1d7ac54c543d> recuperado el 17/05/2020.

[2271] Confr. <https://www.qeh.ox.ac.uk/content/blockchain-refugees-great-hopes-deep-concerns> recuperado el 17/05/2020. Véase también <https://www.wfp.org/news/blockchain-against-hunger-harnessing-technology-support-syrian-refugees> y <https://www.digitaltrends.com/cool-tech/world-food-programme-building-blocks-iris-scanning-blockchain/> disponibles en la misma fecha.

[2272] Confr. <https://www.digitaltrends.com/cool-tech/world-food-programme-building-blocks-iris-scanning-blockchain/> recuperado el 17/05/2020.

[2273] Confr. <https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/> recuperado el 18/05/2020.

[2274] Véase <https://en.blocko.io/about-us/>

[2275] Confr. <https://www.coindesk.com/south-korea-blockchain-community-vote> recuperado el 18/05/2020.

[2276] Confr. <https://www.economist.com/sites/default/files/northeastern.pdf> recuperado el 18/05/2020.

[2277] Confr. <https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf> recuperado el 18/05/2020.

[2278] Confr. <https://www.theverge.com/2020/2/13/21136219/voatz-blockchain-voting-app-election-software-hacking-mit-research-cybersecurity> y en <https://cointelegraph.com/news/blockchain-voting-systems-could-be-the-future-but-current-flaws-persist> recuperado el 18/05/2020.

[2279] Confr. <https://digital.hbs.edu/platform-rctom/submission/smartmatic-the-role-of-blockchain-in-enabling-elections/> recuperado el 18/05/2020.

[2280] Confr. <https://medium.com/bpfoundation/blockchain-applications-election-voting-a1436e7d10cb> recuperado el 18/05/2020. Se recomienda la lectura de la obra de Kevin Curran, *E-voting on the blockchain*, disponible al 18/05/2020 en https://www.researchgate.net/publication/329400689_E-Voting_on_the_Blockchain.

[2281] Véase <https://marketpay.io>

[2282] Confr. <https://www.esmartcity.es/comunicaciones/comunicacion-sistema-votacion-participacion-ciudadana-basado-tecnologia-blockchain> disponible al 07/05/2020.

[2283] Véase *supra* lo dicho en torno al *gas* en la blockchain de Ethereum en la nota 145.

[2284] Confr. Freya Hardwick, Konstantinos Markantonakis y Raja Akram, *Fair and transparent blockchain based tendering framework: A step towards Open Governance*, disponible al 17/05/2020 en https://www.researchgate.net/publication/327479167_Fair_and_Transparent_Blockchain_A_Step_Towards_Open_Governance. Véase también la obra de Bertrand Maltaverne, *What can blockchain do for Public Procurement?* en https://www.publicspendforum.net/blogs/bertrand-maltaverne/2017/08/28/blockchain-technology-public-procurement/?utm_content=buffer0e59e&utm_medium=social&utm_source=twitter.com&utm_campaign=twitter y, del mismo autor, <https://medium.com/procurement-tidbits/blockchain-what-are-the-opportunities-for-procurement-d38cfd5446fa> recuperados el 18/05/2020.

[2285] Confr. Freya Hardwick, Konstantinos Markantonakis y Raja Akram, *Fair and transparent blockchain based tendering framework...o.c.*

[2286] Confr. Jamie Berryhill, Théo Bourgery y Angela Hanson, *Blockchains Unchained: Blockchain Technology and its use in the Public Sector*, recuperado el 18/05/2020 en <https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?>

[expires=1589914680&id=id&accname=guest&checksum=13DDA8B35D7EEBD7491F:](https://www.bennettinstitute.cam.ac.uk/blog/governance-revolution-or-costly-distraction-reasse/)
[2287]

Idem, p. 28.

[2288]

Idem, p. 44.

[2289]

Confr. <https://www.bennettinstitute.cam.ac.uk/blog/governance-revolution-or-costly-distraction-reasse/> recuperado el 18/05/2020.

[2290]

Confr. [Albert Sanchez-Graells, Data-Driven and Digital Procurement Governance: Revisiting Two Well-Known Elephant Tales](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440552), Agosto de 2019, disponible al 18/05/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440552.

[2291]

Confr. <https://gcn.com/articles/2018/11/15/gsa-blockchain-mas.aspx> recuperado el 18/05/2020.

[2292]

Confr. <https://static1.squarespace.com/static/56534df0e4b0c2babdb6644d/t/5cfaa34d5a82320> disponible al 17/05/2020.

[2293]

Confr. <https://www.chilecompra.cl/2018/07/chilecompra-inicia-proyecto-piloto-para-el-uso-de-la-herramienta-blockchain-en-compras-publicas/> recuperado el 18/05/2020.

[2294]

Véase el interesante artículo de Ramanathan Somasundaram y Quamrul Hasan, Asian Development Bank, *Regional: Development of a Global e-Government Procurement Architecture using Blockchain Technology*, disponible al 18/05/2020 en https://www.adb.org/sites/default/files/project-documents/47192/47192-001-tacr-en_5.pdf.

[2295]

Al 18/05/2020 el texto proyectado se encuentra disponible en <http://bases.cortesaragon.es/bases/boca2.nsf/8624462dba822641c12567ad003ec605/b9:OpenDocument>

[2296]

Puede ampliarse en la obra de Miguel Ángel Bernal Blay, *El desarrollo autonómico de la normativa sobre contratos públicos*, disponible al 18/05/2020 en [https://www.google.com/url?](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiRm_ef4uDoAhUIG7kGF)

[sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiRm_ef4uDoAhUIG7kGF](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiRm_ef4uDoAhUIG7kGF)

[2297]

Confr. <https://es.cointelegraph.com/news/argentina-rio-negro-lottery-will-use-blockchain-to-provide-transparency-to-its-processes> recuperado el 17/05/2020.

[2298]

Confr. Comisión Europea, *Blockchain for digital government*, disponible al 18/05/2020 en https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for

[2299] Ampliar en <https://exonum.com/story-georgia> recuperado el 18/05/2020.

[2300] Confr. Comisión Europea, *Blockchain for digital government*, o.c., p. 19. Puede ampliarse en la interesante obra de George Eder, *Digital Transformation: Blockchain and Land Titles*, disponible al 18/05/2020 en https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf.

[2301] Confr. <https://www.reuters.com/article/us-sweden-blockchain/sweden-tests-blockchain-technology-for-land-registry-idUSKCN0Z22KV> recuperado el 18/05/2020.

[2302] Confr. <https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain> recuperado el 18/05/2020.

[2303] Confr. Deloitte, *Blockchain technology and its potential in taxes*, disponible al 17/05/2020 en https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF

[2304] Idem, p. 11.

[2305] Ibid.

[2306] Idem, p. 12.

[2307] Idem, p. 13.

[2308] Confr. <https://www.jdsupra.com/legalnews/austin-s-blockchain-for-the-homeless-64669/> recuperado el 17/05/2020.

[2309] Confr. <https://techcrunch.com/2018/04/14/austin-is-piloting-blockchain-to-improve-homeless-services/> recuperado el 18/05/2020.

[2310] Ibid.

[2311] Confr. Constance E. Bagley, *What's Law got to do with it? a Systems approach to Management*, disponible al 17/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=898652. Afirma Bagley que la *astucia legal* permite y fomenta el diálogo *Legal-to-Management*, una comunicación asertiva y efectiva entre managers y sus asesores legales, un trabajo en conjunto para resolver problemas complejos, integrando las consideraciones legales en la formulación y ejecución de estrategias para proteger y potenciar los recursos de la empresa. La astucia legal es un valioso proceso managerial, una práctica de capacidades dinámicas para acompañar empresas

que construyen ventajas competitivas en un "mundo de competencia Schumpeteriana basada en la innovación, la rivalidad de precios y performance, dividendos crecientes, y la "destrucción creativa" de competencias actuales".

[2312]

Confr. Rob May, *Emerging problems in AI, and Blockchain as a solution*, disponible al 05/05/2020 en <https://hackernoon.com/emerging-problems-in-ai-and-blockchain-as-a-solution-19c04883b642>.

[2313]

Confr. Héctor Alegria, *El Derecho Privado hoy y la innovación jurídica*, LA LEY 29/05/2013, Cita Online: AR/DOC/2014/2013.

[2314]

Confr. Karen Yeung, en *Regulation by blockchain: the emerging battle for supremacy between the Code of Law and Code as Law*, publicado en *Modern Law Review*, Marzo de 2019, Vol. 82, número 2, p. 239.

[2315]

Ibid.

[2316]

Confr. Mark Fenwick, Wulf A. Kaal y Erik Vermeulen, *Legal education in the blockchain revolution*, recuperado el 21/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2939127, p. 5.

[2317]

Idem, p. 6. Sostienen los autores citados, en opinión que se comparte: **"Increasingly, legal work, such as contract drafting, legal risk management, and dispute resolution, will be outsourced to technology and robots. Lawyers and legal advisors will increasingly assume the role of project managers and business advisors."** El resaltado es mío.

[2318]

Véase <https://law.stanford.edu/organizations/pages/legal-design-lab/>

[2319]

Se ha definido a la Economía del Conocimiento como aquella en la que la producción de bienes y servicios está basada en actividades que son intensivas en conocimiento, y que depende en gran medida de capacidades intelectuales, más que de insumos físicos o de recursos naturales. Ampliar en Walter W. Powell y Kaisa Snellman, *The Knowledge Economy*, 2004, recuperado el 01/04/20 de https://scholar.harvard.edu/files/kaisa/files/powell_snellman.pdf.

[2320]

Se recomienda ampliar en Nagi Hanna, *A role for the state in the digital age*, recuperado al 1/04/20 en <https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-018-0086-3>. La autora analiza los casos de Singapur y de la *Smart City* de Wuhan, y propone una serie de principios para la digitalización del Estado.

[2321]

Ampliar en Deloitte Insights, *Forces of change: Industry 4.0*, disponible al 1/04/20 en <https://www2.deloitte.com/es/es/pages/manufacturing/articles/que-es-la->

[industria-4.0.html](#).

[2322]

Confr. <https://www.lanacion.com.ar/el-mundo/martin-wolf-es-una-catastrofe-de-la-que-acaso-no-nos-recuperemos-realmente-por-decadas-nid2349387> disponible a 1/04/20.

[2323]

Confr. <https://www.bbc.com/mundo/vert-earth-39851987>, disponible al 1/04/20, donde se señala que "*como consecuencia del derretimiento del permafrost, los vectores de infecciones mortales de los siglos XVIII y XIX pueden volver, especialmente cerca de los cementerios donde fueron enterradas las víctimas de estas infecciones*".

[2324]

Puede ampliarse sobre el particular en el artículo del autor *Cambio Climático: adaptación, mitigación e impulso a la securitización sustentable*, publicado por Ed. Errepar, Revista Temas de Derecho Comercial, Empresarial y del Consumidor, Mayo 2020.

[2325]

Principalmente, los (enormes!) riesgos relacionados a ciberseguridad, a la privacidad de los datos en una Economía Digital, a la restricción o flexibilización de ciertas libertades individuales en aras de la salud pública, y a los derechos de los consumidores y usuarios en la Economía Digital.

[2326]

Véase el informe de 2016 del Banco Mundial donde se estudian los beneficios sociales en distintos sectores que está produciendo el acceso masivo a Internet, disponible al 04/04/20 en <https://www.worldbank.org/en/publication/wdr2016>.