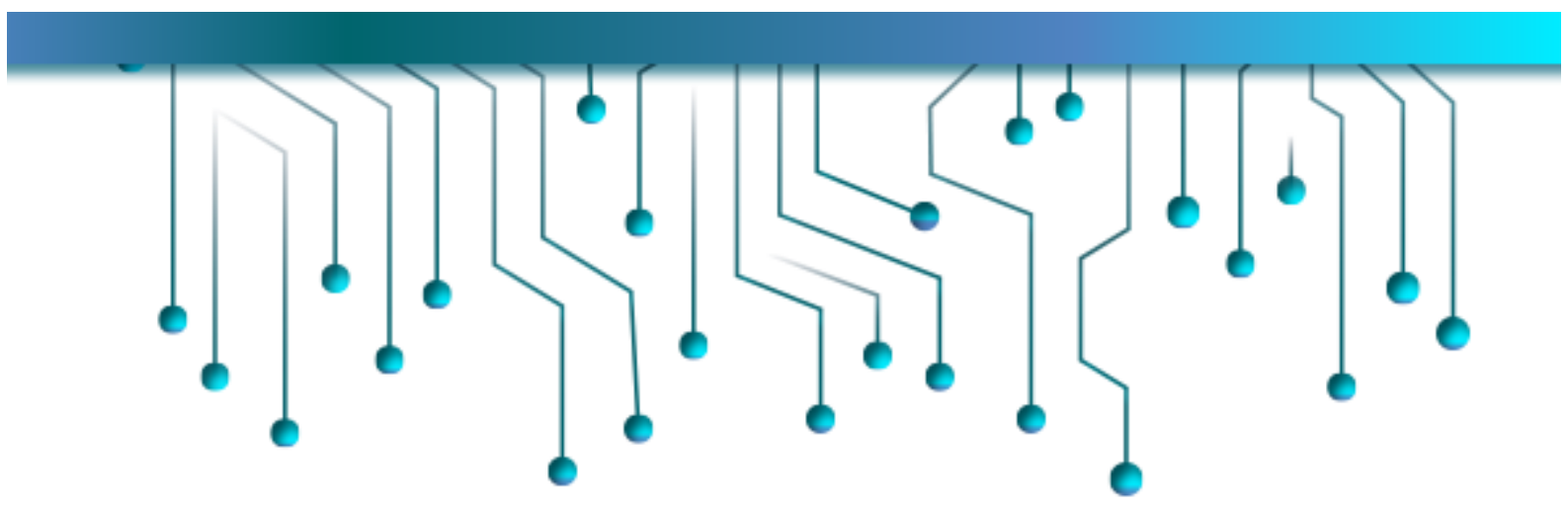


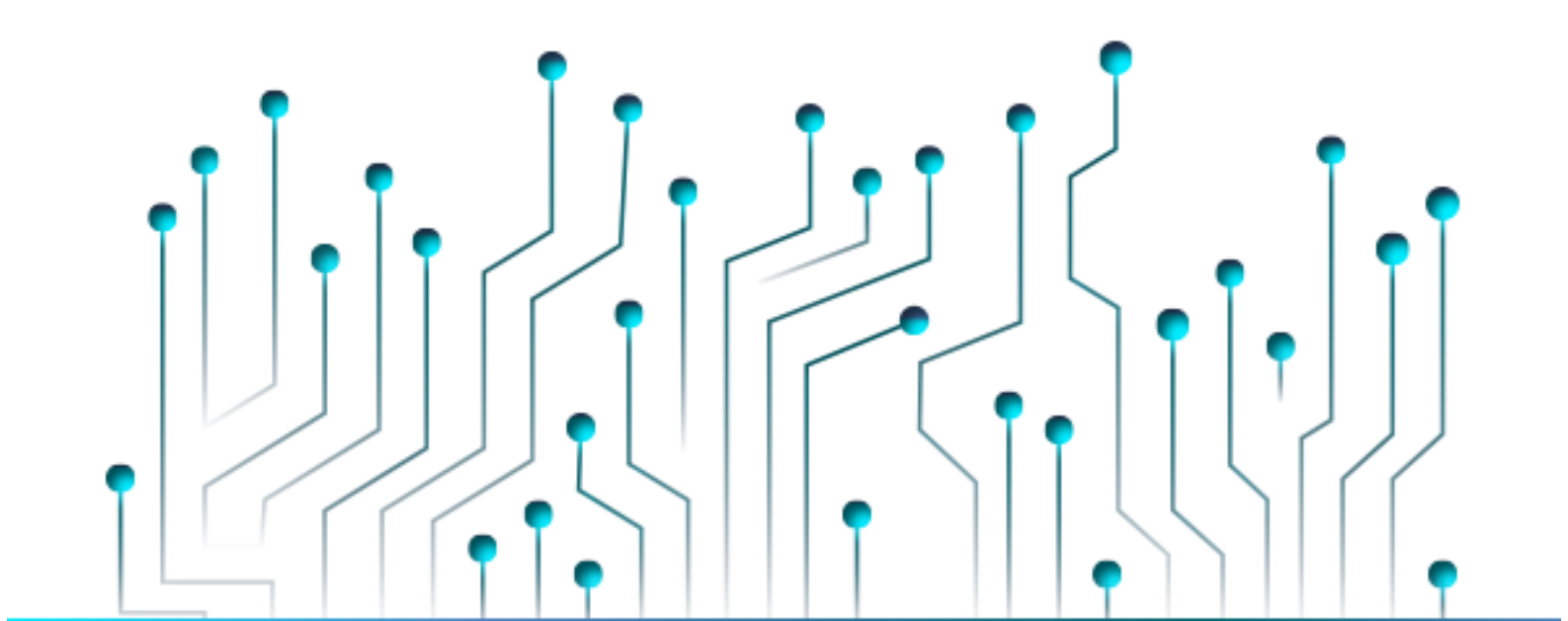


UNIVERSIDAD DE GRANADA
FACULTAD DE DERECHO

TESIS DOCTORAL

BLOCKCHAIN: UN DESAFÍO LEGAL

ANA ISABEL QUIROZ RUIZ



2023



Universidad de Granada



PROGRAMA DE DOCTORADO: CIENCIAS JURÍDICAS

UNIVERSIDAD DE GRANADA

TESIS DOCTORAL

BLOCKCHAIN: UN DESAFÍO LEGAL

D^a. ANA ISABEL QUIROZ RUIZ

**DIRECTORA: DRA. D^a. INMACULADA SÁNCHEZ RUIZ
DE VALDIVIA**

Granada, 2023

Editor: Universidad de Granada. Tesis Doctorales
Autor: Ana Isabel Quiroz Ruiz
ISBN: 978-84-1117-915-7
URI: <https://hdl.handle.net/10481/83004>

A Rafa y a mi madre

Agradecimientos

Gracias a todas y cada una de las personas que han contribuido en la elaboración de esta tesis, en especial a Rafa, porque sin su apoyo incondicional en los momentos más duros, esta tesis no hubiese sido posible. A mi madre que siempre me animó a terminarla. A lunita por ser mi compañera fiel en la soledad de la investigación. A mis hermanos Moni, Toni, Meli, Alejita y Mario. A Mari, por siempre animarme. Gracias a mis amigas, Kat, Ange y Adri que a pesar de la distancia siempre han estado para mí. Así como a Laura, María y Saray.

Especiales y sinceros agradecimientos a la Dra. Inmaculada Sánchez Ruiz de Valdivia por aceptar ser mi directora, por haber comprendido mis tiempos y mi trabajo. Sin su ayuda este trabajo no hubiese sido posible. Su guía, apoyo y paciencia han sido invaluable, por su entera disposición y la facilitación de los medios necesarios para culminarlo.

TABLA DE CONTENIDO

ABREVIATURAS.....	15
INTRODUCCIÓN	20
.....	27
CAPÍTULO UNO: BLOCKCHAIN Y LA LEY.....	29
I. BLOCKCHAIN Y LA LEY.....	29
1. El sueño de Satoshi	29
2. Blockchain: la tecnología y sus características	30
3. De internet a la tecnología Blockchain	33
4. ¿El código es ley?	37
4.1 Implicaciones sociales del código	39
4.2 Saga DAO: el código contraataca.....	41
II. BLOCKCHAIN: UNA TECNOLOGÍA REGULADORA Y REGULABLE	43
1. Preocupaciones, amenazas y riesgos	45
2. Beneficios del código como ley.....	47
3. ¿La nueva <i>lex mercatoria</i> ? - <i>lex criptografía</i>	48
3.1 Desafíos regulatorios de la tecnología Blockchain.....	50
3.2 Cómo regular: formas de abordar la regulación	51
CAPITULO DOS: BLOCKCHAIN Y LOS CONTRATOS INTELIGENTES.....	57
I. LOS CONTRATOS INTELIGENTES.....	57
1. Introducción	57
2. El ascenso de los Smart Contracts	58
II. SMART CONTRACTS Y EL DERECHO CONTRACTUAL.....	62
1. Planteamiento.....	62
2. El contrato inteligente como contrato legal.....	63
2.1 Consentimiento	65
2.2 Objeto	66
2.3 Causa	67
3. Tipos de contratos inteligentes	68
3.1 Contrato escrito y ejecutado íntegramente por el código	68
3.2 Contrato inteligente que tiene un envoltorio en papel	71
3.3 Híbrido: contrato legal tradicional y código.....	73
3.4 Ricardian contract.....	75
4. Contratos legales inteligentes	77
4.1 ¿Cómo deberían ser los contratos inteligentes?.....	78
5. Algunos desafíos jurídicos: errores de codificación	80
5.1 Errores de codificación en Ethereum.....	81

5.2	Sentencia B2C2 vs Quoine	83
5.3	Conclusiones del caso.....	86
6.	Responsabilidad por errores de programación	87
7.	¿Qué sucede con el contrato?	89
III.	CONTRATOS INTELIGENTES EN UNA CADENA DE BLOQUES	94
1.	Introducción.....	94
2.	Concepto de contratos inteligentes.....	95
2.1	Inmutabilidad.....	97
2.2	Autoejecutable	98
2.3	Seudónimo.....	99
2.4	No son tan inteligentes	100
3.	Ethereum	101
4.	Funcionamiento de los contratos inteligentes	104
4.1	Multifirma.....	107
4.2	Oráculo	107
IV.	LENGUAJE DE PROGRAMACIÓN Y LENGUAJE NATURAL.....	109
1.	De la ambigüedad y otros demonios	109
2.	Contratos inteligentes y semántica legal.....	112
2.1	Límites del lenguaje.....	112
2.2	Estudio del lenguaje.....	113
3.	Relación de los lenguajes.....	114
3.1	¿Cómo podemos superar estas limitaciones?	116
4.	Consideraciones finales del lenguaje.....	118
		121
	CAPÍTULO TRES: LA PROTECCIÓN DE LOS CONSUMIDORES DE	
	CRIPTOACTIVOS: RETOS REGULATORIOS	123
I.	LA PROTECCIÓN DE LOS CONSUMIDORES DE CRIPTOACTIVOS:	
	RETOS REGULATORIOS	123
1.	Introducción.....	123
2.	Estafas, pérdidas de dinero y riesgos	130
3.	Implicaciones de la centralización en la protección de los consumidores.	133
II.	ADVERTENCIAS A NIVEL EUROPEO.....	137
1.	Advertencias por parte de autoridades españolas	141
2.	Tratamiento de los criptoactivos en España	143
2.1	Competencias de la CNMV en materia de publicidad	143
2.2	Proyecto de Ley de los Mercados de Valores y de Servicios de Inversión	147
III.	LA PROTECCIÓN DE LOS CONSUMIDORES Y LA PROPUESTA DE	
	REGLAMENTO	148
1.	Introducción.....	148

2.	Respuesta de MiCA para la protección de los consumidores	152
2.1	Concepto de consumidor	152
2.2	Ámbito de aplicación.....	153
2.3	¿Qué se entiende por criptoactivo?.....	153
3.	Ficha referenciada a activo (<i>asset-referenced tokens</i> -ART)	154
4.	Ficha de dinero electrónico (<i>Electronic Money tokens</i> -EMT)	156
5.	Ficha de servicio (<i>Utility token</i>)	157
6.	Proveedores de servicios de criptoactivos	158
7.	Derecho de desistimiento	161
8.	Libro blanco (<i>whitepaper</i>)	162
9.	Procedimiento para la tramitación de reclamaciones	165
10.	Prevención del abuso del mercado	166
11.	Observaciones finales	167
		173
	CAPÍTULO CUATRO: BLOCKCHAIN Y LA RESOLUCIÓN DE DISPUTAS DESCENTRALIZADA	175
I.	JUSTICIA DESCENTRALIZADA: RESOLUCIÓN DE DISPUTAS EN BLOCKCHAIN	175
1.	Introducción	175
2.	Resolución de Controversias en Blockchain	177
3.	Resolución de controversias en línea (ODR)	178
4.	Resolución de disputas descentralizada y distribuida	181
4.1	Teoría de juegos.....	183
4.2	Crowdsourcing.....	186
4.3	Inteligencia colectiva	187
II.	PLATAFORMAS DE RESOLUCION DE CONFLICTOS DE GESTION COLABORATIVA EN BLOCKCHAIN	188
1.	Mecanismos alternativos de resolución de disputas colaborativo (CODR) 188	
1.1	Kleros.....	188
1.2	Aragon Court	191
1.3	Rhubarb	192
2.	Plataformas de Arbitraje en Blockchain	194
2.1	Jur	195
2.2	Juris.....	199
2.3	CodeLegit	201
2.4	Mattereum.....	203
2.5	OpenCourt	204
3.	Jurisdicción Distribuida	205
III.	DESAFIOS DE LAS PLATAFORMAS DE RESOLUCIÓN DE CONFLICTOS BASADAS EN BLOCKCHAIN	206

1. Desafíos CODR	206
1.1 Selección de los jurados	207
1.2 Justicia	207
1.3 Ejecución, vinculación y legalidad	210
2. Desafíos del Arbitraje.....	211
2.1 Reconocimiento y ejecución.....	212
2.2 Costos	214
3. Consideraciones	215
.....	219
CAPITULO QUINTO: BLOCKCHAIN Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.....	221
I. BLOCKCHAIN Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.....	221
1. Introducción	221
2. Definición de dato personal a la luz del RGPD.....	222
2.1 Toda información.	224
2.2 La información debe versar sobre una persona	225
2.3 La persona ha de estar identificada o identificable.....	226
2.4 Persona física	228
3. Anonimización y seudonimización	229
3.1 Anonimización.....	229
3.2 Seudonimización	233
II. DATOS ALMACENADOS EN BLOCKCHAIN.....	234
1. Función <i>Hash</i>	235
1.1 Función <i>hash</i> en Blockchain.....	238
1.2 La función <i>hash</i> y su función en el almacenamiento de datos en Blockchain. ¿Puede la función hash anonimizar datos?	239
2. Clave pública - criptografía asimétrica	244
2.1 Criptografía asimétrica en Blockchain	245
2.2 ¿Las claves públicas son datos personales?	246
III. DESAFÍOS DE LOS DERECHOS DE LOS INTERESADOS.....	255
1. Derecho al olvido en Blockchain	256
1.1 Derecho de supresión (el derecho al olvido)	257
1.2 ¿Qué significa supresión?	259
1.3 Soluciones técnicas.....	263
1.4 Consideraciones.....	268
2. Derecho de rectificación	269
IV. TENSION Y PRINCIPIOS MINIMIZACIÓN DE DATOS Y LIMITACIÓN DEL PLAZO DE CONSERVACIÓN	271
V. RESPONSABLE DEL TRATAMIENTO.....	273
1. Desarrolladores	275
2. Mineros	276

3. Nodos.....	277
3.1 Corresponsables del tratamiento.....	279
3.2 Consideraciones acerca de los nodos.....	281
CONCLUSIONES	286
I. Blockchain y la ley.	286
II. Blockchain y los contratos inteligentes	288
III. La protección de los consumidores de criptoactivos: retos regulatorios ...	292
IV. Blockchain y resolución de disputas descentralizada.....	298
V. Blockchain y el Reglamento General De Protección De Datos.....	300
.....	308
BIBLIOGRAFÍA	309
Webgrafía	364
Recursos multimedia	370
Anexo de jurisprudencia	370
Anexo de legislación.....	372
España.....	372
Europa	373
Otros países	374

ABREVIATURAS

ABE	Autoridad Bancaria Europea
ADR	Alternative Dispute Resolution
AEPD	Agencia Española de Protección de Datos
AESPJ	Autoridad Europea de Seguros y Pensiones de Jubilación
AML	Anti-Money Laundering
ANT	Aragon Network Token
ART	Asset-Referenced Tokens
BOE	Boletín Oficial del Estado
BTC	Bitcoin
CEPD	Comité Europeo de Protección de Datos
CODR	Crowdsourced Online Dispute Resolution
CNMV	Comisión Nacional del Mercado de Valores
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DCFR	Draft Common Frame of Reference
DeFi	Decentralized Finance
DORA	Digital Operational Resilience for The Financial Sector and Amending Regulations
EDI	Electronic Data Interchange
EMT	Electronic Money Tokens
ESMA	European Securities and Markets Authority
ETH	Ether
ICO	Initial Coin Offering

IOSCO	Organization of Securities Commissions
JERS	Junta Europea de Riesgo Sistémico
KYC	Know your Customer
LSSICE	Ley de Servicios de la sociedad de la información y de comercio electrónico
MiCA	Markets in Crypto-Assets
NFT	Non-Fungible Token
RAL	Resolución Alternativas De Litigios
RGPD	Reglamento General de Protección de Datos
RLL	Resolución de Litigios en Línea
SEPD	Supervisor Europeo de protección de datos
SESF	Sistema Europeo de Supervisión Financiera
TJUE	Tribunal de Justicia de la Unión Europea
TOR	The Onion Router
TRD	Tecnología de Registros Distribuidos
UE	Unión Europea
UNIDROIT	Institut International Pour L'unification Du Droit Privé

INTRODUCCIÓN

INTRODUCCIÓN

El desarrollo tecnológico ha puesto de manifiesto la necesidad que tiene el derecho de adaptarse a las nuevas tecnologías. Supuestamente, Blockchain¹, la tecnología subyacente de Bitcoin, está llamada a ser el desarrollo más importante en tecnología de la información desde la aparición de internet², por lo que su desarrollo impactará de una u otra forma en la aplicación del derecho.

Blockchain, es como un registro de datos descentralizado y distribuido que registra la información de forma transparente, permanente e inalterable. “Es, en definitiva, un gigantesco libro contable donde se apuntan (registran) todas y cada una de las transacciones o transferencias realizadas es capaz de almacenar toda la información que jamás se podrá perder, modificar o eliminar”³. Las transacciones que se depositan se realizan mediante un mecanismo de consenso y criptografía. Permite a personas que no se conocen entre sí, llegar a un acuerdo sin la necesidad de un intermediario. Esta tecnología ha permitido el desarrollo de Smart Contracts⁴, acuerdos de naturaleza anónima que se ejecutan automáticamente sin la necesidad de intervención humana. Los contratos inteligentes, según sus defensores, ofrecen la posibilidad de ahorro de costos legales, de transacción y una mayor eficiencia comercial. Con la aparición de estos contratos, han surgido una serie de preocupaciones en torno a su naturaleza jurídica, en si son realmente inteligentes; así como su adaptación al sistema normativo y el impacto positivo o negativo que su uso pueda generar en la contratación. Estos acuerdos, así como la cadena de bloques en sí misma, representan una serie de desafíos legales a los que el derecho debe dar respuestas.

Los contratos inteligentes que se ejecutan en Blockchain, parecen tener el potencial de proporcionar una mayor eficiencia que los contratos tradicionales, pues, supuestamente reducen los costos legales y de transacción, eliminando gran parte de los

¹ Cadena de bloques en español.

² WERBACH, K. (2018). "Trust, But Verify: Why the Blockchain Needs the Law", *Berkeley Technology Law Journal*, vol. 33, no. 489, pp. 489. Disponible en: <https://papers.ssrn.com/abstract=2844409> (fecha de consulta: 18 de julio de 2019).

³ SÁNCHEZ RUIZ DE VALDIVIA, I. (2020). “Blockchain e inteligencia artificial: dos tecnologías que convergen e impactan en la economía y el derecho”, *Blockchain: impacto en los sistemas financiero, notarial, registral y judicial*, (Dirs. SANCHEZ RUIZ DE VALDIVIA, I.). Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra. pp. 58 y ss.

⁴ Contratos inteligentes en español.

gastos que genera la presencia de intermediarios en este tipo de transacciones. Para su cumplimiento no es necesaria la intervención humana, porque se ejecutan de acuerdo a lo estipulado en el código. La tecnología subyacente, dado su carácter inmutable, garantiza que el acuerdo no sea modificado. Todos estos aparentes beneficios suponen al mismo tiempo preguntas y preocupaciones en torno a su legalidad, practicidad y las consecuencias que su uso pueda generar.

A través de estos contratos, las partes pueden diseñar sus propias cláusulas, que serán ejecutadas dentro de la red Blockchain siempre y cuando se cumplan las condiciones que fueron programadas en el código, pero ¿Ello puede permitir la aplicación de normas privadas contrarias o paralelas al ordenamiento jurídico? ¿El código es la ley? ¿Pueden los acuerdos privados basados en Blockchain regular la ley? ¿El uso de contratos inteligentes reelaborará el derecho contractual tradicional? Hay quienes, como DE FILIPPI y WRIGHT⁵ consideran que, con las cadenas de bloques, las personas pueden construir sus propios sistemas de reglas o contratos inteligentes, ejecutados por el protocolo subyacente de una red basada en Blockchain. Señalan que estos sistemas crean orden sin ley, e implementan lo que se puede considerar como marcos regulatorios privados a los que denominan *lex criptografía*, que prescinden de las leyes tradicionales y se basan en el código informático para coordinar y regular el comportamiento humano.

Autores como WERBACH⁶, que advierten: (i) los contratos inteligentes automatizan la aplicación contractual al ceder todo el poder a la red descentralizada de Blockchain, advirtiendo que todo lo que está más allá del código, es solo una explicación y que, si bien la automatización del cumplimiento genera ciertos beneficios y tiene el potencial de eliminar el sistema legal de la ejecución contractual, estos tipos de acuerdo no pueden plasmar en su código conceptos subjetivos como “mejores esfuerzos” o “razonabilidad” – principios que, dicho sea de paso, se encuentran en la base del Derecho contractual europeo más moderno- por lo que las partes afectadas terminarán recurriendo a los tribunales.

⁵ DE FILIPPI, P. & WRIGHT, A (2018). *Blockchain and the Law The Rule of Code*, Harvard University Press, United State Of America, pp. 7-8.

⁶ WERBACH, K. (2018). "Trust, But Verify: Why ...", *Cit.*, pp. 529.

Igualmente, en la doctrina se ha venido discutiendo la protección de los consumidores en este entorno, pues al ser una tecnología que opera entre pares y sin intermediarios, en principio, las partes estarían en igualdad de condiciones. No obstante, la ausencia de intermediarios ha supuesto un problema para las partes débiles, pues la presencia de estos se ha vuelto casi que imprescindible para la adopción de esta tecnología por parte del gran grueso de la población. En este sentido, la industria de criptoactivos se ha desarrollado sin un régimen legal aplicable (dado que se trata de nuevas formas de inversión), que por lo menos brinde unas salvaguardias mínimas a los consumidores.

Otro desafío jurídico asociado al empleo de Blockchain es la resolución de controversias, pues dada su naturaleza distribuida, Blockchain se desarrolla en múltiples ubicaciones, por lo que se plantean problemas jurisdiccionales y de ley aplicable. De igual forma, el seudonimato genera problemas prácticos para individualizar a las partes, de manera que se dificulta incoar acciones jurídicas. CASINO⁷ afirma que, debido a la naturaleza ubicua de las disputas, se debe proporcionar una gestión eficiente de conflictos que supere los costos transfronterizos e institucionales. Como respuesta, se han creado aplicaciones tecnológicas como métodos de resolución de disputas descentralizados para Blockchain, los cuales se basan en la teoría de juegos, como método de incentivo económico, sabiduría de las multitudes, y sistemas de colaboración abierta y distribuida. Si bien el desarrollo y diseño de estas aplicaciones son una respuesta práctica y novedosa desde la propia tecnología, no están exentos de preocupaciones y problemas en torno a su concepción de justicia y la forma como se resuelven las disputas al margen del estado de derecho.

En este orden de ideas, otro aspecto preocupante a tener en cuenta, es lo relativo a la protección de los datos personales. Si bien el Reglamento General de Protección de datos⁸ es una norma tecnológicamente neutral, se concibió con un control central en mente, lo que choca con la naturaleza descentralizada de las cadenas de bloques. Asimismo, la transparencia de las redes públicas supone que cualquier persona pueda

⁷ CASINO, F., DASAKLIS, T.K. y PATSAKIS, C. (2019). "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, Vol. 36, pp. 55-81. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0736585318306324> (fecha de consulta: 20 de octubre de 2021).

⁸ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

visualizar el historial de las transacciones. Un bloque en Blockchain almacena, entre otros datos, las direcciones de sus participantes y la carga útil, que contiene la información cifrada sobre la transacción, los cuales pueden considerarse como datos personales. Ello significa que es imprescindible la identificación del responsable del tratamiento, pues es ante quien recae las obligaciones contenidas en el RGPD y es ante quien los interesados deben acudir para ejercer derechos como el de rectificación u olvido. De igual forma, la inmutabilidad representa obstáculos para la aplicación estos derechos, así como el cumplimiento de principios como la minimización de datos y limitación del plazo de conservación.

A la vista de lo esbozado en párrafos anteriores, esta tesis busca reflexionar en profundidad y dar respuesta sobre estos y otros desafíos jurídicos que representa la implementación de la de la tecnología Blockchain para el derecho. Examinamos si la revolución a la que invita esta tecnología exigirá que repensemos los modelos legales existentes. Para ello, nos enfocaremos en el estudio de las cadenas de bloques públicas, habida cuenta de que para las cadenas bloques privadas y con permiso es menos problemático ajustarse a las normas legales.

Se trata de una investigación jurídica, con un enfoque cualitativo y de carácter analítico-descriptivo. Los conocimientos hallados se emplearon para el estudio del régimen jurídico aplicable a las cadenas de bloques. Se realizó un rastreo bibliográfico de diferentes investigaciones doctrinales nacionales e internacionales, con el objetivo de comprender, analizar y adquirir conceptos integrales en relación con los desafíos jurídicos de Blockchain. Debido a su carácter jurídico, esta investigación no profundiza en cuestiones técnicas de la tecnología Blockchain. En este sentido, solo se abordan cuando son estrictamente necesarios para la comprensión de la misma.

Las técnicas de recolección de la información se basaron en un análisis documental con fuentes de carácter primario y secundario como artículos, monografías, ensayos, jurisprudencia, *whitepaper*, entre otros. Estas fuentes se recolectaron a través de bases de datos como Web Of Science, Scopus, Dialnet, Google Scholar, sciELO y de repositorios institucionales como SSRN, JSTOR y arXiv.

El desarrollo de esta tesis, se encuentra estructurado en 5 capítulos. El primer capítulo, se ocupa de describir, a modo de introducción, los orígenes y funcionamiento de la tecnología Blockchain, la interacción del código y la ley, es decir, el código y su capacidad de regular el comportamiento de las personas, a través de su arquitectura, que permite o restringe determinadas acciones. Asimismo, se explora la posibilidad de regulación de esta tecnología, dada su naturaleza distribuida y descentralizada.

Por su parte, el segundo capítulo, reflexiona sobre si los Smart Contracts constituyen o no acuerdos legales, en este sentido, y tras analizar la legislación civil sobre la formación de los contratos y, determinar que depende de la tipología de cada uno, procedemos analizarlos individualmente. Asimismo, examinamos la problemática que subyace de la autoejecución del código, las implicaciones en caso de que haya errores de programación y los inconvenientes de la inflexibilidad del código en los acuerdos contractuales como fenómenos sociales.

El tercer capítulo, examina la desprotección de los consumidores frente a la industria de los criptoactivos, un sector que ha evolucionado sin un marco regulatorio específico, lo que ha representado una serie de peligros y riesgos para los pequeños inversores. No obstante, como respuesta a esta problemática la Unión Europea presentó a finales del 2020 una propuesta de Reglamento para regular parte de este sector, por lo que analizamos las medidas introducidas para la protección de los consumidores.

El capítulo cuarto, aborda la resolución de disputas descentralizada. Se expone que Blockchain no elimina la presencia de desacuerdos entre las partes. Se analizan los aspectos legales y prácticos de ocho plataformas de resolución de conflictos que emplean la tecnología de la cadena de bloques. Se estudia la viabilidad jurídica de la adopción de los mecanismos y herramientas utilizadas por estas plataformas para resolver conflictos.

Finalmente, el capítulo quinto, se ocupa de los desafíos que supone para Blockchain el Reglamento General De Protección De Datos. Se delimita el concepto de dato personal y a partir de ahí se analiza si el empleo de la clave pública y la función *hash* constituyen o no datos personales a la luz del RGPD. De igual forma, se evalúa los desafíos de los derechos de los interesados y la tensión entre los principios de

minimización de datos y limitación del plazo de conservación y, por último, se intenta identificar al responsable del tratamiento de datos en una Blockchain pública.

CAPÍTULO UNO

BLOCKCHAIN Y LA LEY

CAPÍTULO UNO: BLOCKCHAIN Y LA LEY

I. BLOCKCHAIN Y LA LEY

1. El sueño de Satoshi

Las bases ideológicas de Blockchain, la tecnología subyacente de la criptomoneda Bitcoin, se remontan al movimiento libertario anarcocapitalista conocido como “ciberpunk”, el cual defiende la privacidad y la libertad de expresión mediante la criptografía, firmas electrónicas, sistemas de envío anónimo de e-mail y dinero electrónico⁹. De este movimiento surgiría el manifiesto *criptoanarquista*¹⁰, escrito por TIM MAY en 1996, quien acuñó una nueva forma de anarquía, definida como *criptoanarquía*¹¹. En este manifiesto se describe que gracias a la tecnología criptográfica se alteraría la capacidad de regulación de los gobiernos.

Unos años más tarde, el 31 de octubre de 2008, en plena crisis financiera mundial, SATOSHI NAKAMOTO publicaba el *Whitepaper* de Bitcoin¹², una criptomoneda independiente de cualquier autoridad central o tercero intermediario, que solucionaba el problema del doble gasto. Su publicación se hizo a tan solo medio mes de la quiebra de Lehman Brothers y de otros gigantes financieros como AIG (*American International Group*), que se salvaron gracias a la intervención por parte de autoridades gubernamentales.

Como una reacción al colapso financiero, que ya había presentado sus primeros síntomas con la crisis de las hipotecas *Subprime* en 2007, SATOSHI NAKAMOTO presentaba Bitcoin como “una solución descentralizada a un problema causado por la sobrecentralización”¹³. Bitcoin era, de alguna forma, un sueño de devolverle el control a

⁹ HUGHES, E. (1993). “A Cypherpunk's Manifesto”. Disponible en: <https://www.activism.net/cypherpunk/manifesto.html> (fecha de consulta: 1 de diciembre de 2019).

¹⁰ MAY, T. (1994). “Manifiesto criptoanarquista”. Disponible en: <https://www.mises.org/es/2017/02/manifiesto-criptoanarquista/> (fecha de consulta: 20 de noviembre de 2019).

¹¹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 1.

¹² NAKAMOTO, S. (2008). “Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer”. Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf (fecha de consulta: 2 de abril de 2019).

¹³ BAIR, T. (2019). “How Decentralized Tech Can End the Privacy Crisis in 2020”. Disponible en: <https://www.coindesk.com/how-decentralized-tech-can-end-the-privacy-crisis-in-2020> (fecha de consulta: 5 de enero de 2020).

las personas y, a su vez, una forma de protesta y una alternativa contra un sistema financiero defectuoso, que paradójicamente fue rescatado cuando los gobiernos le inyectaron capital a los mismos bancos que habían causado la crisis, mientras que los propietarios que incumplieron con las hipotecas recibieron solo ayudas limitadas¹⁴.

Unos tres meses más tarde, el 3 de enero de 2009, SATOSHI NAKAMOTO extraía el bloque génesis de Bitcoin, el cual contiene la siguiente frase: “03/Ene/2009 Canciller a punto del segundo rescate para los bancos¹⁵”. Este mensaje fue sacado de la edición impresa de ese día del periódico Time del Reino Unido, no solo para probar que la moneda se había minado ese día, sino que también representaba un fuerte mensaje político en contra de la banca y los bancos centrales.

2. Blockchain: la tecnología y sus características

Mundialmente conocida por ser la tecnología subyacente de Bitcoin, aunque su uso va más allá de la industria de la criptomonedas y finanzas, como por ejemplo, los contratos inteligentes o la trazabilidad de las cadenas de suministro, Blockchain (Cadena de Bloques), también conocida como tecnología de contabilidad distribuida (DLT)¹⁶, es un libro mayor compartido, distribuido e inmutable, protegido mediante criptografía, que facilita el proceso de registro y rastreo de transacciones¹⁷, lo que significa que es un registro descentralizado, de igual a igual, en el cual los participantes que contribuyen a la red pueden verificar y confirmar las transacciones sin necesidad de una autoridad central.

Cada nodo de la red posee una copia del libro mayor, el cual se va actualizando a medida que se producen nuevas transacciones. Un nodo es una computadora, por lo que

¹⁴ WERBACH, K. (2018). *The blockchain and the new architecture of trust*, The MIT Press, Cambridge, Massachusetts, p. 38.

¹⁵ El mensaje original de time era: “Chancellor Alistair Darling on brink of second bailout for banks”, que hacía referencia a que el entonces ministro de hacienda del Reino Unido Alistair Darling, tenía que decidir si seguir inyectando capitales a los bancos del Reino Unido.

¹⁶ FEIGN, A. (2022). “What Is Blockchain Technology?”. Disponible en <https://www.coindesk.com/learn/what-is-blockchain-technology/> (fecha de consulta: 2 de diciembre de 2022).

¹⁷ IBM. (Sin fecha) “What is blockchain technology?”. Disponible en: <https://www.ibm.com/topics/what-is-blockchain> (fecha de consulta: 2 de diciembre de 2022).

la cadena de bloques está compuesta por muchos ordenadores conectados entre sí¹⁸, “esto crea una especie de telaraña mundial de computadoras conectadas”¹⁹.

Como su nombre lo indica, Blockchain está conformada por bloques enlazados cronológicamente. Los bloques son estructuras de datos que almacenan información acerca de la transacción²⁰, como, por ejemplo, la hora en la cual se efectuó. Cada bloque que integra la cadena está relacionado mediante *hash* con el bloque anterior²¹, por lo cual, para hacer cualquier modificación, se necesita del consenso de la mayoría de nodos. En otras palabras, “el *hash* del bloque anterior vincula los bloques entre sí e impide que se altere cualquier bloque o que se inserte un bloque entre dos bloques existentes. De este modo, cada bloque posterior refuerza la verificación del bloque anterior y, por tanto, de toda la cadena de bloques”²². Este mecanismo, es lo que hace a Blockchain a prueba de manipulaciones y, en consecuencia, inmutable.

Para verificar las transacciones y añadir un nuevo bloque a la cadena, se emplea un mecanismo de consenso, lo que significa que todos los nodos deben estar de acuerdo sobre su validez, que dependiendo del diseño puede ser, entre otros, de prueba de trabajo (POW, por sus siglas en inglés *Proof of Works*) o prueba de participación (POS, por sus siglas en inglés *Proof of Stake*).

- i. La prueba de trabajo es el mecanismo de consenso detrás de Bitcoin y resuelve el problema del doble gasto, ya que en el mundo digital es muy fácil copiar y pegar un archivo²³. Este procedimiento suele llamarse minería y los nodos que

¹⁸ KOMALAVALLI, C., SAXENA, D., & LAROIYA, C. (2020). “Chapter 14 - Overview of Blockchain Technology Concepts” *Handbook of Research on Blockchain Technology* (Dirs. KRISHNAN, S., BALAS, V., JULIE, E., ROBINSON, Y., BALAJI, S. & KUMAR, S.), Ed.: Academic Press, pp. 871-903. Disponible en: <https://www.sciencedirect.com/science/article/pii/B9780128198162000149> (fecha de consulta: 17 de noviembre de 2022).

¹⁹ SABRINA, A. (2022). “Blockchain: La tecnología de cadena de bloques”. Disponible en: <https://criptoescultura.com/tecnologia-cadena-de-bloques/> (fecha de consulta: 2 de diciembre de 2022).

²⁰ SIMÕES, C. (2022). “¿Qué son los bloques en la tecnología Blockchain?”. Disponible en: <https://www.itdo.com/blog/que-son-los-bloques-en-la-tecnologia-blockchain/> (fecha de consulta: 27 de noviembre de 2022). Para profundizar detalladamente los tipos de datos que se almacenan en el bloque véase el capítulo IV sección II de la presente obra.

²¹ Un hash es una función matemática que transforma cualquier dato de longitud variable en una salida de tamaño fijo, véase el Capítulo quinto, sección II, donde se aborda con más detalle este concepto.

²² GUPTA, M. (2018). *Blockchain For Dummies*, John Wiley & Sons, Inc., p. 14. Disponible en: <https://www.ibm.com/downloads/cas/36KBMBOG> (fecha de consulta: 12 de octubre de 2022).

²³ HERTIG, A. (2022). “What Is Proof-of-Work?”. Disponible en: <https://www.coindesk.com/learn/2020/12/16/what-is-proof-of-work/> (fecha de consulta: 27 de noviembre de 2022).

participan en él se conocen como mineros. Para agregar un nuevo bloque, los mineros deben competir entre ellos y resolver un rompecabezas matemático para averiguar el valor *hash* del bloque siguiente²⁴. El minero que resuelva primero el puzzle será quien agregue el bloque y recibirá una recompensa por ello. Para resolver dicho rompecabezas se necesita de mucha potencia informática, lo que requiere de muchos recursos energéticos.

- ii. Por su parte, la prueba de participación, recientemente adoptada por Ethereum, en un proceso conocido como *The Merge* (La Fusión)²⁵. Es una alternativa de ahorro de energía de la prueba de trabajo²⁶. En este algoritmo a los nodos que participan se les conoce como validadores. Se trata de un mecanismo en el cual, para validar las transacciones, los validadores deben realizar “una participación, un depósito de tokens, para tener la oportunidad de acabar elegidos para aprobar transacciones y obtener una pequeña recompensa”²⁷, de tal forma que para participar los nodos necesitan invertir en la moneda. En Ethereum, por ejemplo, se exige a los validadores para poder participar de un mínimo de 32 ETH, unos 40 mil euros²⁸.

Actualmente, existen diferentes tipos de cadenas de bloques: públicas, privadas y de consorcio. Las Blockchain públicas son aquellas en las que cualquier persona (sin necesidad de permiso) puede ver y convertirse en un nodo y participar en el mecanismo de consenso. Un ejemplo de este tipo de redes son Bitcoin o Ethereum.

Las cadenas de bloques privadas son aquellas que están administradas por una sola entidad quien administra la red y determina los permisos a los usuarios que desean participar²⁹ en el mecanismo de consenso. En este tipo de redes, aunque los participantes

²⁴ YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain technology overview*, National Institute of Standards and Technology, Gaithersburg, pp. 9 y ss. Disponible en: <https://doi.org/10.6028/NIST.IR.8202> (fecha de consulta: 7 de septiembre de 2021).

²⁵ The merge se implementó en Ethereum el 14 de septiembre de 2022.

²⁶ ZHENG, Z., XIE, S., DAI, H., CHEN, X., & WANG, H. (2017). “An overview of blockchain technology: Architecture, consensus, and future trends”, *IEEE international congress on big data*. Disponible en: https://ieeexplore.ieee.org/abstract/document/8029379?casa_token=XfECS0v33zkAAAAA:EYB6h2tf8JBG8alHltwMWpJE8XBYJ7DgdQG4zAqy4lfmMEpY8NzKvJPnc0kegBmmn7L6dzsx2TA (fecha de consulta: 1 de noviembre de 2021).

²⁷ ACKERMANN, R. (2022). “Ethereum abandona la criptominería y adopta la prueba de participación”, *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/14589/ethereum-abandona-la-criptomineria-y-adopta-la-prueba-de-participacion> (fecha de consulta: 23 de noviembre de 2022).

²⁸ Precio del Ether para el 14 de diciembre de 2022.

²⁹ ALLENDE, M. (2018). ¿Pública, federada o privada? Explora los distintos tipos de blockchain”. Disponible en: <https://blogs.iadb.org/conocimiento-abierto/es/tipos-de-blockchain/> (fecha de consulta: 2 de diciembre de 2022).

guarden una copia local de la información, no existe descentralización. Un ejemplo de este tipo de cadenas sería Hyperledger.

Por último, las Blockchains de consorcio, son una combinación entre cadenas de bloques públicas y privadas³⁰. En este tipo de redes no se permite que cualquier nodo participe en el mecanismo de consenso, porque estos han sido previamente escogidos, pues forman parte de las empresas que conforman el consorcio. Su diferencia con respecto a las cadenas de bloques públicas estriba en que no es un sistema abierto en el que cualquiera se puede unir para validar bloques, y con respecto a las privadas, es que no es un sistema cerrado en el que solo una parte selecciona a los nodos que harán parte del mecanismo de consenso³¹. En este tipo de redes solo un pequeño número de nodos actuarán como validadores. Un ejemplo de este tipo de Blockchain sería Corda del consorcio R3³².

3. De internet a la tecnología Blockchain

Cuando internet se empezó a consolidar en la década de los noventa, suscitó ideales de anarquía e ilegalidad³³, convirtiéndose en el objetivo de los utópicos liberales³⁴. Internet fue vista como una plataforma independiente que permitiría la libertad de los individuos, al margen de cualquier control estatal, y eliminaría la regulación mediante la descentralización³⁵. Incluso se sumaron voces que esgrimían que el ciberespacio crearía sus propias leyes e instituciones legales³⁶.

³⁰ “Blockchains Privadas, Públicas y de Consorcios - ¿En qué se diferencian?”. (2021). Disponible en: <https://academy.binance.com/es/articles/private-public-and-consortium-blockchains-whats-the-difference> (fecha de consulta: 23 de noviembre de 2022).

³¹ SINGH, J. (2021). “Private, public and consortium”. Disponible en: https://cointelegraph.com/explained/private-public-and-consortium-blockchains-the-differences-explained?_ga=2.78093074.749293923.1671180305-1403019528.1663574162 (fecha de consulta: 22 de noviembre de 2022).

³² “R3” (Sin fecha). Disponible en: <https://www.r3.com/corda-platform/> (fecha de consulta: 16 de junio de 2020).

³³ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 7.

³⁴ LESSIG, L. (2009). *El código 2.0*, Traficantes de sueños, Madrid, p. 32.

³⁵ WERBACH, K. (2018). “Trust, But Verify: Why ...”, cit., p. 522.

³⁶ JOHNSON, D. R. POST, D. G. (1996). “Law and Borders –The Rise of Law in Cyberspace”, Stanford Law Review, vol. 48. p. 1367. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535&download=yes (fecha de consulta: 20 de diciembre de 2019).

Nadie mejor que JOHN PERRY BARLOW, cofundador de *Electronic Frontier Foundation*³⁷ para reflejar esta visión, pues en la *Declaración de Independencia del Ciberespacio*, afirmó que, los gobiernos “No ejercéis ninguna soberanía sobre el lugar donde nos reunimos” (...) “ni poseéis métodos para hacernos cumplir vuestra ley que debamos temer verdaderamente”³⁸, a lo que añadió que “Los conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican”³⁹.

Estas predicciones jamás se cumplieron, los sueños ciberlibertarios se fueron desvaneciendo, a medida que internet fue madurando, pasando de ser un espacio de anarquía a un espacio fuertemente regulado⁴⁰. Si bien, en la arquitectura original⁴¹ de la red, la reglamentación era difícil, pues esta “estaba diseñada para difundir información de la manera más rápida y libre posible, evitando las interceptaciones en un nodo concreto”⁴², esta fue modificada para permitir su regulación⁴³. Como GOLDSMITH y WU⁴⁴ explicaron, el diseño de internet fue moldeado por los caprichos y obsesiones de los gobiernos poderosos de los Estados Unidos, China y Europa, logrando implantar su mandato a la actividad en línea.

³⁷ Advierten en la doctrina GOLDSMITH, J. & WU, T. (2006). *who controls the internet? illusions of a borderless world*, Oxford University Press, Inc., que Barlow junto con John Gilmore y Mitch Kapor fundaron Electronic Frontier Foundation, fundación sin ánimo de lucro que se dedica a desarrollar y defender las libertades civiles y la idea del ciberespacio como un lugar separado de cualquier estado.

³⁸ BARLOW, J. P. (2009). “Declaración de independencia del ciberespacio.” *Periférica Internacional. Revista para el análisis de la cultura y el territorio*, Vol. 1, No. 10, p. 241. Disponible en: <https://revistas.uca.es/index.php/periferica/article/view/943> (fecha de consulta: 29 de septiembre de 2019).

³⁹ BARLOW, J. P. (2009). “Declaración de...”, *cit.*, 241.

⁴⁰ Para una excelente explicación acerca del control de los gobiernos sobre internet, véase la obra completa de GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, *Op. Cit.* Incluso LESSIG, L. (2009). *El código 2...*, *Op. Cit.*, p. 486, advierte que el “ciberespacio pasaría de ser un espacio irregulable a ser (...) el espacio más regulable que se pueda imaginar”.

⁴¹ Al respecto GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, *Op. Cit.*, p. 22, afirman que, la primera arquitectura de internet fue desarrollada principalmente por académicos y empleados de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) del departamento de defensa de los Estados Unidos con fines de investigación y gubernamentales. El modelo TCP/IP (Protocolo de control de transmisión/Protocolo de Internet), también conocido como el protocolo de internet, fue concebido como una arquitectura abierta que, en palabras de Goldsmith Y Wu, era un diseño que desconfiaba del control centralizado.

⁴² PUERTO, M.J. (2007). “La regulación de Internet y la teoría jurídica”, *Anuario de filosofía del derecho*, No. 24, p. 444. Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=2769990> (fecha de consulta: 5 de enero de 2020).

⁴³ LESSIG, L. (2009). *El código 2...*, *Op. Cit.*, p. 468. Para profundizar y entender las razones que dieron forma a los protocolos de internet véase CLARK, D. (1988). “The design philosophy of the DARPA internet protocols | Symposium proceedings on Communications architectures and protocols”, *Computer Communication Review*, Vol. 18, No. 4, pp. 106-114. Disponible en <https://dl.acm.org/doi/abs/10.1145/52324.52336> (fecha de consulta: 1 de noviembre de 2019).

⁴⁴ GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, *Op. Cit.*, p. 72

Los Estados⁴⁵ encontraron la forma de regular la actividad en línea, porque si bien internet era ubicua (al igual que Blockchain), necesitaba de la existencia de terceros para poder funcionar, y al contrario de lo que se creyó inicialmente, los intermediarios no se eliminaron, sino que cambiaron⁴⁶. Los proveedores de servicios de internet (*ISP*, por sus siglas en inglés), proveedores de *hosting*, motores de búsqueda, fabricantes de *hardware*, etc., hicieron posible en gran parte la regulación de la red, pues permitieron a los reguladores un punto de control al estar sometidos a las leyes de la jurisdicción del lugar donde se hallaban⁴⁷.

Hoy en día, las visiones libertarias han desaparecido casi por completo. Internet no solo aumentó el poder de los gobiernos para vigilar el comportamiento de sus ciudadanos⁴⁸, sino también el de las grandes empresas, así como una concentración de poder por parte de estas corporaciones. Como ya advirtieron, con acierto, DE FILIPPI y WRIGHT en 2018, “la aparición de teléfonos móviles, tiendas de aplicaciones y plataformas de computación en la nube ha llevado al establecimiento de una red más centralizada, dominada por un puñado de corporaciones que controlan el flujo de información y las transacciones económicas”⁴⁹.

Incluso los regímenes totalitarios descubrieron que podían utilizar la red como una herramienta útil para el monitoreo y la represión.⁵⁰ Países como Irán, Arabia Saudita y China⁵¹, han implementado *firewalls* (cortafuegos, en español) que censuran y bloquean contenido que consideran sensible⁵². El *firewall* construido por China se conoce como el

⁴⁵ Gran parte de esa regulación se hizo gracias al comercio, ver detalladamente LESSIG, L. (2009). *El código 2...*, Op. Cit., quien hace una excelente explicación al respecto.

⁴⁶ GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, Op. Cit., p. 70.

⁴⁷ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a regulatory technology: From code is law to law is code", *First Monday*, Vol. 21, No. 12, p. 9. Disponible en: <https://doi.org/10.5210/fm.v21i12.7113> (fecha de consulta: 16 de marzo de 2019).

⁴⁸ GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, Op. Cit., p. 84.

⁴⁹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 8.

⁵⁰ WERBACH, K. (2018). "Trust, But Verify: Why ...", cit., p. 523.

⁵¹ Afirma FREEDOM HOUSE. (2018). *Freedom on the net 2018: The rise of digital authoritarianism*, p. 6. Disponible https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf (fecha de consulta: 5 de enero de 2020), que otros países con políticas similares son: Venezuela, Cuba, Egipto, Etiopía, Rusia, Turquía, Afganistán, Pakistán, Corea del Norte, Tailandia, Vietnam, entre otros.

⁵² Explican DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (2007). *Access Denied the Practice and Policy of Global Internet Filtering*, MIT Press, Cambridge, p. 5, que un sistema de filtrado está destinado a evitar que los ciudadanos comunes accedan a algunas partes de Internet que el estado considera demasiado sensibles, por una razón u otra. La información bloqueada abarca desde política hasta sexualidad, cultura y religión.

gran cortafuegos, (*Great Firewalls*, en inglés) o la gran muralla China, constituyéndose como “el sistema de filtrado más grande y sofisticado del mundo”⁵³. Sin embargo, no solo regímenes totalitarios o países con democracias débiles censuran información, particularmente Europa y Estados Unidos filtran contenidos que violan derechos de propiedad intelectual⁵⁴ y sitios de pornografía infantil⁵⁵.

Independientemente de si se posee un interés legítimo para censurar, ello definitivamente significa que internet no es un lugar libre. Baste, como muestra, el reporte de FREEDOM HOUSE de 2018 “*Freedom on the net*”⁵⁶, en el que se advertía que la libertad global de internet disminuyó por octavo año consecutivo en 2018 y que la democracia misma se está debilitando bajo su influencia.

Lo interesante de todo esto es que ilustra cómo se utiliza el código informático para regular el comportamiento en línea de las personas. Si bien los gobiernos pudieron utilizar la ley tradicional para alcanzar sus objetivos, optaron hacerlo mediante la arquitectura técnica de la red, y ello se debió, en gran parte, a que el código es más efectivo y menos percibido que ley, “parece más una fuerza de la naturaleza que un ejercicio de poder político o físico”⁵⁷. Por ejemplo, cuando alguien en China intenta acceder a un sitio web censurado por el gobierno chino, no le aparecerá un mensaje de bloqueo, sino que puede experimentar un tiempo de espera largo⁵⁸ o un mensaje de error, adquiriendo una apariencia de error técnico⁵⁹.

⁵³ DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (2007). *Access Denied the...*, Op. Cit., p. 263. Ver también LEE, J. & LIU, C. (2012). “Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China”, *Minnesota Journal of Law, Science, and Technology*, Vol. 13, No.1. Disponible en: <https://papers.ssrn.com/abstract=2035788> (fecha de consulta: 20 de diciembre de 2019).

⁵⁴ Según el informe FREEDOM HOUSE. (2018). *Freedom on the net...*, Op. Cit., p. 4, de 65 países analizados (representan el 87% de los usuarios de internet del mundo), 26 países tuvieron una disminución de la libertad en la red y solo 19 presentaron mejoras, siendo estas mismas menores.

⁵⁵ Véase la obra completa de DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (2007). *Access Denied the...*, Op. Cit. Estos autores realizan en este libro un excelente análisis sobre las políticas de filtrado y bloqueo de internet en varios países alrededor del mundo.

⁵⁶ FREEDOM HOUSE. (2018). *Freedom on the net...*, Op. Cit., p. 1.

⁵⁷ DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (2007). *Access Denied the...*, Op. Cit., p. 3.

⁵⁸ Véase “Los grandes muros de seguridad que los países están construyendo en Internet”. (2016). Disponible en: <https://www.xataka.com/tecnologiaz/los-grandes-muros-de-seguridad-que-los-paises-estan-construyendo-en-internet> (fecha de consulta: 5 de enero de 2020).

⁵⁹ GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, Op. Cit., p. 94.

Recientemente, el advenimiento de la tecnología Blockchain y los contratos inteligentes han revivido esos sueños ciberlibertarios de los orígenes de internet. Blockchain, según sus defensores, representa un enorme potencial de innovación en las finanzas, la contratación y el comercio. Se ha planteado que por ser una tecnología distribuida y descentralizada puede carecer del estado como autoridad central y ser no regulable. Pero ¿pueden estas tecnologías no ser regulables y funcionar al margen de la intervención estatal? Blockchain es todavía una tecnología en desarrollo, y todo parece indicar que está recorriendo un camino similar al internet en relación con la ley.

Internet demostró que el código se podía someter a la ley, lo que sugiere que las empresas y los gobiernos no se dejarán desintermediar tan fácilmente. Cuando estos actores desearon regular, encontraron la forma de hacerlo⁶⁰ y ello se debió, en parte, a la presencia de intermediarios y a la naturaleza rastreable de las direcciones IP⁶¹, de tal manera que, si Blockchain presenta puntos de control parecidos a los de internet, la labor reguladora será más fácil.

Sin embargo, a pesar de tener estos puntos en común con Internet, habrá que superar una serie de desafíos legales debido al carácter “anónimo”⁶² y a la ausencia de un punto de control⁶³. Con lo cual, la regulación de la tecnología Blockchain será todo un reto, aunque no imposible. Por ello la pregunta no es si ¿se puede o no regular?, sino ¿cómo hacerlo?

4. ¿El código es ley?

Desde el surgimiento del internet, el vínculo entre el código y la ley ha sido el centro de múltiples discusiones, destacándose en el debate la premisa “el código es la ley”, que significa que el código y la arquitectura del ciberespacio pueden producir

⁶⁰ WERBACH, K. (2018). "Trust, But Verify: Why ...", *cit.*, p. 524. Para entender por qué los fenómenos tecnológicos actuales siguen siendo los mismos desafíos legales que planteó internet cuando se comercializó en los años noventa, véase WERBACH, K. 2018, "The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy", *Florida Law Review*, Vol. 69, pp. 887-957.

⁶¹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 68.

⁶² En realidad, Blockchain es seudónimo, esta cuestión se aborda detalladamente en el capítulo quinto, título I, apartado 3.2.

⁶³ YEUNG, K. (2019) "Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law", *The moder Law Review*, Vol. 82, No. 2, p. 237. Disponible en: <https://ssrn.com/abstract=3347280> (fecha de consulta: 25 de octubre de 2019).

efectos similares a la ley⁶⁴. Es decir, el código como regulador de la conducta en el espacio digital, en lugar de la ley tradicional, siendo “capaz de restringir las acciones de un individuo por medios tecnológicos”⁶⁵.

Esta frase fue popularizada por el profesor LESSIG en 1999, siendo la hipótesis principal del libro, *el código y otras leyes del ciberespacio*. LESSIG tomó esta idea de WILLIAM MITCHEL quien defendía que el “código es la ley del ciberespacio”⁶⁶, pero que prefirió resumir en “el código es la ley”⁶⁷.

La arquitectura técnica de cualquier plataforma depende del diseño elegido por sus desarrolladores, que buscan admitir o restringir determinadas conductas, de tal manera que sus atributos establecen que se puede o no hacer en el entorno digital; mucho más que la ley aplicable, más efectivo⁶⁸, e incluso mucho más estricto⁶⁹.

A este tipo de reglas se les denomina gobernanza, que es la programación introducida por los propietarios de las plataformas y que, por lo general, salvaguardan sus intereses privados⁷⁰. Por ejemplo, considere visualizar una película o serie en una plataforma de streaming como Netflix o HBO, es el código técnico el que determina desde qué lugar o dispositivo se puede acceder, quién puede hacerlo o si es posible descargar el

⁶⁴ KAESEBERG, T. (2019). "The Code-ification of Law and Its Potential Effects", *Stanford Journal of blockchain law and policy*, Vol. 2, No. 2 Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535&download=yes (fecha de consulta: 20 de diciembre de 2019). Véase también a REIDENBERG, J. (1996). "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, No. 76. Disponible en: https://ir.lawnet.fordham.edu/faculty_scholarship/42 (fecha de consulta 1 de noviembre de 2019), quien la denominó *Lex Informatica*.

⁶⁵ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a...", *cit.*, p. 4

⁶⁶ MITCHELL, W. (1995). *City of Bits: Space, Place, and the Infobahn*, Cambridge, MIT Press, p. 111, como se citó en LESSIG, L. (2001). *El código y otras leyes del ciberespacio*, Santillana, Madrid, p. 25.

⁶⁷ Señala en la doctrina LESSIG, L. (2001). *El código y otras ...*, *Op. Cit.*, p. 25, que no solo se basó en las ideas de Mitchell, sino que también se inspiró en otros autores como KATSH, E (1996). "Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace", *University of Chicago Legal Forum*, pp. 335, 338 y También en la obra de Reidenberg quien la denominó *Lex Informatica* en REIDENBERG, J. (1996). "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, No. 76. Disponible en: https://ir.lawnet.fordham.edu/faculty_scholarship/42. (fecha de consulta 1 de noviembre de 2019).

⁶⁸ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a...", *cit.*, p. 2

⁶⁹ WERBACH, K. (2018). "Trust, But Verify: Why ...", *cit.*, p. 536.

⁷⁰ GOVERNMENT OFFICE FOR SCIENCE. (2016). *Distributed ledger technology: Blackett review. Distributed ledger technology: Beyond block chain*, UK Government Chief Scientific Adviser. Disponible en: <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>. (fecha de consulta: 20 de septiembre de 2019). Ver también LEHDONVIRTA, V. (2016,). The blockchain paradox: Why distributed ledger technologies may do little to transform the economy. Disponible en: <https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/> (fecha de consulta: 5 de enero de 2020).

contenido multimedia. La forma en la que esa arquitectura restringe o permite ese comportamiento depende de las decisiones que adopte su programador (propietario).

No obstante, la idea de que el código es ley no representa que el código sea igual que la ley, “lo que LESSIG quiso decir era que la arquitectura de internet, su *hardware* y *software*, eran una forma diferente y potencialmente poderosa para controlar el comportamiento en internet”⁷¹. Las normas legales se podían incorporar en el código, y este a su vez, podía ser regulado por las empresas y las autoridades. “Porque el código no es la ley, como tampoco lo es el diseño de un avión”⁷². En este sentido, el código regula mejor o de forma más efectiva el comportamiento, que las normas tradicionales, no obstante, el código no es ni debería ser la ley.

4.1 Implicaciones sociales del código

El espectro de posibilidades y limitaciones de comportamiento que permite el código, tiene efectos reguladores de facto⁷³; lo que significa que el diseño de arquitecturas técnicas puede terminar promoviendo o inhibiendo determinados valores sociales⁷⁴.

Desde los años ochenta se ha venido argumentando que ciertas tecnologías en sí mismas tienen propiedades políticas⁷⁵ que favorecen algunas acciones más que otras, lo que implica que la tecnología no es neutral⁷⁶, pues al estar diseñada por humanos, refleja sus valores e ideas⁷⁷. Piense, por ejemplo, cuando un programador va a diseñar un *software*, este debe tomar determinadas decisiones sobre su funcionamiento y acerca de

⁷¹ GOLDSMITH, J. & WU, T. (2006). *who controls the internet...*, *Op. Cit.*, p. 72.

⁷² LESSIG, L. (2009). *El código 2...*, *Op. Cit.*, p. 505

⁷³ HILDEBRANDT, M. (2019). *Law for Computer Scientists and Other Folk*, Oxford University Press, p. 15. Disponible en: <https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g> (fecha de consulta: 18 de enero de 2020).

⁷⁴ SURDEN, H. (2017) "Values Embedded in Legal Artificial Intelligence", *University of Colorado Law School Legal Studies Research Paper Series*, No. 17-17. Disponible en: <https://ssrn.com/abstract=2932333> (fecha de recuperación 20 de enero de 2020).

⁷⁵ WINNER, L. (1980). "Do Artifacts Have Politics?", *Daedalus*, Vol. 109, No. 1, p. 123. Disponible en: <https://www.jstor.org/stable/20024652?origin=JSTOR-pdf&seq=1> (fecha de consulta: 2 de enero de 2020).

⁷⁶ Según MOWSHOWITZ, A. (1984). "Computers and the myth of neutrality", *Proceedings of the ACM 12th annual computer science conference on SIGCSE symposium*, p. 86. Disponible en: <https://dl.acm.org/doi/10.1145/800014.808144> (fecha de consulta: 2 enero de 2020), Los artefactos tienen una historia social y están dotados de propósitos humanos. El diseño, la producción y la difusión constituyen una red social compleja que admite relativamente poca libertad de elección individual.

⁷⁷ WEBER, R.H. (2018). "“Rose is a rose is a rose is a rose” – what about code and law?", *Computer Law & Security Review*, Vol. 34, No. 4, p. 703. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918301882> (fecha de consulta: 2 de abril de 2019).

qué acceso y restricciones tendrán los usuarios. En principio, puede parecer que estas elecciones son neutrales, pero su diseño dicta qué acciones se pueden hacer o no hacer.

En la doctrina, LANGDON WINNER argumenta que estas decisiones puede que no hayan sido una elección consciente, o puede que hayan sido intencionalmente elegidas, como los puentes sobre las avenidas de Long Island en Nueva York, cuyos pasos elevados fueron deliberadamente diseñados de esa forma para obtener un determinado efecto social. El diseño demasiado bajo de los puentes (9 pies de altura), obedece a los sesgos clasistas y prejuicios raciales de su arquitecto, ROBERT MOSES, que los diseñó así para evitar el acceso a los vehículos de transporte público (12 pies de altura), impidiendo así que las personas pobres y negras, que normalmente utilizaban este tipo de transporte no tuvieran acceso a las playas públicas, porque los autobuses de 12 pies de altura no podían transitar por los pasos elevados⁷⁸.

Por todo esto, si las decisiones de los programadores reflejan sus valores, teniendo así importantísimas implicaciones sociales, que permiten o limitan determinados comportamientos, o favorecen o perjudican ciertos grupos sociales. Ello sugiere que le prestemos más atención a las características del código y al significado de esas características⁷⁹, porque el papel regulador del código puede tener efectos sobre los derechos de las personas. Como dijo LESSIG “Los códigos constituyen los ciberespacios; los espacios favorecen o perjudican a los individuos y a los grupos. Las decisiones acerca del código representan, en consecuencia, decisiones acerca de quién, qué y, lo más importante, qué formas de vida se verán favorecidas y perjudicadas”⁸⁰.

El lenguaje de Turing completo que se ha desarrollado en las cadenas de bloques, ha permitido la creación de contratos inteligentes que se ejecutan automáticamente en la red subyacente de Blockchain. Cuando un Smart Contract se ejecuta, si se cumplen las condiciones programadas en su código, significa que las reglas no se interpretan, sino que "someten la conducta humana al gobierno de las reglas"⁸¹. Teniendo en cuenta que las tecnologías incorporan valores y políticas en su diseño, lo que tiene importantes

⁷⁸ WINNER, L. (1980). "Do Artifacts Have...", *cit.*, pp. 122-125.

⁷⁹ Véase MOWSHOWITZ, A. (1984). "Computers and the...", *cit.*, pp. 85 y ss.

⁸⁰ LESSIG, L. (2009). *El código 2...*, *Op. Cit.*, p. 155.

⁸¹ DIVER, L. (2018). "Law as a User: Design, Affordance, and the Technological Mediation of Norms", *SCRIPTed*, Vol. 15, No. 1. Disponible en: <https://script-ed.org/?p=3534> (fecha de consulta: 2 de 2020).

implicaciones sociales, esto probablemente requerirá de debates, para que estas nuevas tecnologías con potenciales efectos reguladores permanezcan bajo el Estado de derecho⁸².

4.2 Saga DAO: el código contraataca

La arquitectura de la cadena de bloques de Ethereum ha incluido funcionalidades que permiten la escritura de “*scripts*” (códigos) que pueden ejecutarse automáticamente si se cumplen las condiciones programadas. Las transacciones se ejecutan de forma descentralizada o distribuida en la red de nodos de Blockchain.

Con esto, hemos descrito de forma muy sencilla cómo trabaja un contrato inteligente, pero lo relevante para este punto, es que en su código se pueden incorporar cláusulas contractuales que se ejecutan de forma automática y absoluta, lo que garantiza el cumplimiento de sus reglas. Debido a la inmutabilidad de la cadena de bloques, una vez puesto en marcha el código, este no se puede modificar o detener, a menos que las partes hayan acordado las condiciones previstas para detener o modificar la ejecución del programa⁸³.

La capacidad de ejecución inevitable de los contratos inteligentes es lo que ha llevado a equiparar a estos como la propia Ley⁸⁴, pues lo que dice el código, es lo que se ejecuta. Por supuesto, hay lugar para ciertas preocupaciones, porque sus defensores afirman que, “cualquier error o vulnerabilidad accidental se convierte en parte del contrato también. La explotación de estos errores para controlar activos no se consideraría robo, porque el error que permite la retirada forma parte del código y, por lo tanto, por definición, está dentro de la «ley»”⁸⁵.

Prueba de ello, es el ataque a la DAO (Organización Autónoma Descentralizada en español) en 2016. Una DAO, es una combinación de contratos inteligentes⁸⁶, que se ejecutan automáticamente en una cadena de bloques. Son un tipo de organización que se

⁸² HILDEBRANDT, M. (2019). *Law for Computer Scientists...*, ..., Op. Cit., p. 15.

⁸³ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 75.

⁸⁴ Señalan BOUCHER, P., NASCIMENTO, S., & KRITIKOS, M. (2017). *Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques*. Brussels: European Parliament, p. 15, que es una interpretación radical igualar al código con la ley.

⁸⁵ BOUCHER, P., NASCIMENTO, S., & KRITIKOS, M. (2017). *Cómo puede cambiar nuestra...*, Op. Cit., p. 15.

⁸⁶ WEBER, R.H. (2018). ““Rose is a rose is a rose...””, cit., p. 704.

apoyan en reglas basadas en códigos y otros medios de sistemas algorítmicos e inteligencia artificial para su gobernanza⁸⁷. La DAO⁸⁸ de 2016, fue un sistema de crowdfunding, el mayor de la historia, pues recaudó el equivalente a más de 117 millones de dólares en Ether entre unas 11.000 mil personas alrededor del mundo⁸⁹. Estas personas confiaron en una empresa virtual y sin existencia legal⁹⁰. Su objetivo era financiar los proyectos que fueran elegidos por los titulares, sin necesidad de intermediarios⁹¹. Según la información suministrada por el sitio web que, promocionada la DAO, los términos y condiciones estarían controlados y determinados en la codificación del contrato inteligente, por lo que todas las acciones se registrarían única y exclusivamente por el Código⁹², pues este tomaría el lugar de la ley (el código es ley).

Sin embargo, antes de que empezara a financiar proyectos sucedió algo interesante. Una persona logró desviar 50 millones de dólares a su cuenta. Según una carta abierta publicada por el atacante, no se trataba de un robo, sino de una acción completamente legítima, pues, la función estaba codificada en los términos del contrato inteligente⁹³.

Ethereum no tenía forma de detener el robo, por lo que la comunidad, luego de intensos debates, votó por una bifurcación dura (*hard fork*, en inglés) para que las personas afectadas recuperaran sus fondos, dando origen a Ethereum Classic.

El código de la DAO se ejecutó exactamente para lo que fue diseñado, para reemplazar la aplicación de la ley⁹⁴, lo que evidenció los riesgos que puede desencadenar que el código tome el lugar de la ley, porque un sistema que dependa enteramente del algoritmo representa grandes riesgos para los derechos de las personas y no deberían

⁸⁷ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 4.

⁸⁸ La DAO es el nombre de una DAO particular, concebida y programada por el equipo detrás del startup alemana Slock.it. Ver más información en SIEGEL, D. (2019). "Understanding The DAO Attack" Disponible en: <https://www.coindesk.com/understanding-dao-hack-journalists> (fecha de consulta: 19 de diciembre de 2019).

⁸⁹ Véase PRISCO, G. (2016). "The DAO Raises More Than \$117 Million in World's Largest Crowdfunding to Date" Disponible en: <https://bitcoinmagazine.com/articles/the-dao-raises-more-than-million-in-world-s-largest-crowdfunding-to-date-1463422191> (fecha de consulta: 19 de diciembre de 2019).

⁹⁰ WERBACH, K. (2018). "Trust, But Verify: Why ...", cit., p. 494.

⁹¹ AST, F. (2017). "El DAO: Breve Historia de la Primera Organización Descentralizada". Disponible en: <https://medium.com/astec/el-dao-breve-historia-de-la-primera-organizaci%C3%B3n-descentralizada-e85980f99787> (fecha de consulta: 23 de diciembre de 2019).

⁹² YEUNG, K. (2019) "Regulation by Blockchain...", cit., p. 234.

⁹³ Ver carta escrita por el atacante en "An Open Letter". (2016). Disponible en: <https://pastebin.com/CcGUBgDG> (fecha de consulta: 18 de diciembre de 2019).

⁹⁴ WERBACH, K. (2018). "Trust, But Verify: Why ...", cit., p. 495.

dejarse íntegramente al *software*⁹⁵. Las garantías legales se encargan de corregir fallas y asimetrías, incluso si no se incorpora en el contrato, ya que su aplicación es obligatoria. Por ello, el código se debe someter al régimen legal.

II. BLOCKCHAIN: UNA TECNOLOGÍA REGULADORA Y REGULABLE

Algunos teóricos han argumentado que Blockchain puede impulsar cambios en la forma en que funcionan las normas legales⁹⁶, ya que la cadena de bloques junto con los contratos inteligentes se puede emplear no solo para implementar las leyes en el código, sino también para redactar y elaborar normas legales⁹⁷, es decir, confiar en el código de los contratos inteligentes para regular la conducta de las personas. La llegada de los contratos inteligentes permitiría la aplicación de reglas basadas en códigos que la red de Blockchain ejecutaría automáticamente según lo programado.

En este sentido, y según indican DE FILIPPI Y WRIGHT en su libro de 2018, *Blockchain and the law*, los reguladores podrían utilizar las cadenas de bloques como un medio para aplicar sus propias leyes de manera más eficiente y automática⁹⁸, así como en su tiempo se adoptaron las oportunidades brindadas por internet.

En efecto, las autoridades de algunos países están explorando estas posibilidades, por ejemplo, la OFICINA GUBERNAMENTAL PARA LA CIENCIA DEL REINO UNIDO, en un informe de 2016 sobre tecnología Blockchain, advirtió que “la regulación pública podría ejercerse a través de una combinación de código legal y técnico, en lugar de a través del código legal como en la actualidad. En esencia, el código técnico podría usarse para asegurar el cumplimiento del código legal y, al hacerlo, reducir los costos del cumplimiento legal”⁹⁹.

⁹⁵ YEUNG, K. (2019) "Regulation by Blockchain...", *cit.*, p. 235.

⁹⁶ MILLARD, C. (2018). "Blockchain and law: Incompatible codes?", *Computer Law & Security Review*, Vol. 34, No. 4, pp. 843-846. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918302437> (fecha de consulta: 26 de abril de 2019). Advierte FERNANDEZ, L. (2018). “Diez claves para entender qué es el 'regtech'”. Disponible en: <https://tinyurl.com/y55q8vpw> (fecha de consulta: 20 de febrero de 2020) que, el termino Regtech fue teorizado por primera vez por la Financial Conduct Authority (FCA) véase

⁹⁷ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a...", *cit.*, p. 3.

⁹⁸ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 192.

⁹⁹ GOVERNMENT OFFICE FOR SCIENCE. (2016). *Distributed ledger technology...*, *Op. Cit.*, p. 12.

La plataforma Blockchain CORDA del consorcio R3 es un ejemplo¹⁰⁰ de Regtech basado en tecnología Blockchain. CORDA es un libro de contabilidad distribuido¹⁰¹, de código abierto, que tiene entre sus propósitos permitir nodos de supervisión y regulación¹⁰². El *Whitepaper* de la plataforma explica que, se trata de una arquitectura que está diseñada para modelar y automatizar transacciones de una manera legalmente exigible. A diferencia de las cadenas de bloques públicas, está diseñada para administrar transacciones del mundo real entre partes que son inidentificables, de forma privada y con seguridad jurídica¹⁰³. Los contratos inteligentes que se ejecutan en la plataforma tienen un contrato legal de respaldo¹⁰⁴, por tal razón, son legalmente exigibles en caso de disputa¹⁰⁵, de manera que en caso de un conflicto son las leyes y jueces, no el código, quienes resolverán la disputa. Desestimando afirmaciones como el “código es la ley”¹⁰⁶.

Inicialmente, la plataforma estuvo conformada por instituciones financieras, pero luego se fueron sumando organizaciones de otras industrias e incluso oficinas reguladoras como el Departamento de Regulación Financiera y Profesional de Illinois, quienes se aliaron no solo para explorar los potenciales uso de la tecnología, sino también para buscar la manera de reducir el fraude en las transacciones financieras¹⁰⁷.

¹⁰⁰ YEUNG, K. (2019) "Regulation by Blockchain...", *cit.*, p. 231.

¹⁰¹ A Corda no se le considera propiamente una cadena de bloques, de hecho, no utiliza la prueba de trabajo, sino que funciona mediante un consenso distribuido. Para más información sobre cómo trabaja CORDA vease HEARN, M., & BROWN, R.G (2019). "Corda: A distributed ledger". Disponible en: https://docs.corda.net/_static/corda-technical-whitepaper.pdf (fecha de recuperación: 21 de noviembre de 2019).

¹⁰² BROWN, R.G (2016). "Introducing r3 corda™: a distributed ledger designed for financial services". Disponible en: <https://gandal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/> (fecha de consulta: 21 de noviembre de 2019).

¹⁰³ BROWN, R.G (2018). "The corda platform: An introduction". Disponible en: <https://www.corda.net/content/corda-platform-whitepaper.pdf> (fecha de consulta: 21 de noviembre de 2019).

¹⁰⁴ R3 (2017). "Other Concepts - Legal Prose" Disponible en: <https://vimeo.com/213879293> (fecha de consulta 12 de enero de 2020).

¹⁰⁵ BROWN, R.G., CARLYLE, J.R., GRIGG, I. y HEARN, M. (2016). "Corda: An Introduction". Disponible en: <https://www.corda.net/content/corda-platform-whitepaper.pdf> (fecha de consulta: 21 de noviembre de 2019).

¹⁰⁶ SHEARMAN-STERLING, LLP, R3 & BAFT. (2018). "Code Is Not Law: The Legal Background for Trade Finance Using Blockchain". Disponible en: <https://r3.com/reports/code-is-not-law-the-legal-background-for-trade-finance-using-blockchain/> (fecha de consulta: 17 de noviembre de 2019).

¹⁰⁷ IRRERA, A. (2017). "Illinois watchdog first U.S. regulator to join blockchain consortium R3" Disponible en: <https://www.reuters.com/article/us-blockchain-illinois-idUSKBN16N2FN> (fecha de consulta: 12 de enero de 2020).

1. Preocupaciones, amenazas y riesgos

Por supuesto, existen riesgos y beneficios que deben tenerse en cuenta a la hora de utilizar la tecnología Blockchain para regular la sociedad.

- i. *Errores en el código.* Blockchain y los contratos inteligentes, como cualquier otra tecnología, no es perfecta y es propensa a que existan errores en su código de programación¹⁰⁸. Por ejemplo, a los contratos inteligentes de Ethereum se les han encontrado fallos. En este sentido, cualquier fallo puede desencadenar en una consecuencia catastrófica, véase por ejemplo el caso de la DAO¹⁰⁹ en 2016 que sufrió un ataque informático y se perdieron millones de dólares.
- ii. *Opacidad en el código.* Uno de los riesgos más importantes de la regulación por código es la opacidad acerca de su diseño. Como bien explica LESSIG, “se puede generar el riesgo de invisibilizar la propia regulación. Pese a que los controles impuestos responden a razones políticas concretas, la gente los experimenta como si fuesen naturales”¹¹⁰, lo que evidentemente, pone en duda la transparencia de estos mecanismos, pues estarían permitiendo o restringiendo nuestras actuaciones a través de algoritmos y no sabríamos cómo los reguladores o las compañías privadas deciden y moldean nuestras acciones.
- iii. *Ausencia de procesos democráticos.* La regulación mediante código suele ser deliberada y carente de procesos democráticos. La mayoría de desarrolladores privados de *software* toman las decisiones de manera autocrática, es decir, que no incorpora en sus reglas las opiniones o cuestionamientos de los usuarios (esto particularmente se observa en código cerrado); lo que ha dado pie a que doctrinantes, como HASSAN y DEFILIPPI afirmen que, el sistema legal garantiza la existencia de un conjunto público, transparente y explícito de reglas

¹⁰⁸ véase ORCUTT, M. (2018). "Ojo, los contratos inteligentes de Ethereum están llenos de fallos", *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/10049/ojo-los-contratos-inteligentes-de-ethereum-estan-lenos-de-fallos> (fecha de consulta: 2 de agosto de 2019). Esta cuestión se aborda con más detenimiento en el capítulo dos, título II, apartado 5 de la presente tesis.

¹⁰⁹ En este sentido afirma RODRIGUES, U. (2019). "Law and the Blockchain", *Iowa Law Review*, Vol. 104, No. 2, p. 683. Disponible en: <https://ilr.law.uiowa.edu/print/volume-104-issue-2/law-and-the-blockchain/> (fecha de consulta: 16 de abril de 2019), que, debido a una falla en el código de la DAO, un individuo desconocido pudo desviar alrededor de \$ 50 millones en una cuenta privada.

¹¹⁰ LESSIG, L. (2009). *El código 2...*, Op. Cit., pp. 232-233.

universales, cuya legitimidad puede ponerse en duda fácilmente¹¹¹ en los procesos democráticos¹¹², exigiéndole responsabilidades a nuestros reguladores. De manera que “Si el código se erige en legislador, entonces debería abrazar los principios de los procesos legislativos”¹¹³. La regulación por código es opaca y elimina las garantías constitucionales y la base democrática de la regulación tradicional. Por ejemplo, en el caso de Bitcoin, a pesar de la creencia popular de ausencia de control centralizado, el código de Bitcoin, como cualquier otro, debe ser mantenido y actualizado constantemente. Si bien el código es abierto y cualquiera puede sugerir cambios, la autoridad técnica que admite esos cambios en la versión oficial del *software* está en manos la fundación Bitcoin.

iv. Carácter determinista. El código de un contrato inteligente se ejecutará si se cumplen ciertas condiciones en la red de nodos de Blockchain, de forma automática y absoluta. En principio, esto implica seguridad jurídica; sin embargo, las circunstancias pueden cambiar y ese cumplimiento puede producir resultados imprevistos o indeseables, porque el código no es flexible¹¹⁴. Por esta razón, las partes débiles como los consumidores podrían perder ciertas protecciones legales, así como tampoco el código tampoco podría distinguir entre casos normales y extremos, que necesiten un tipo diferente de tratamiento¹¹⁵.

Las normas legales son deliberadamente genéricas y ambiguas para que tengan la flexibilidad de adaptarse a circunstancias no previstas, es decir, que con estas características se garantiza la aplicación de la ley de forma general y su adecuación a cada caso concreto. En contraste, “cuando un programador crea un programa, predetermina sus respuestas a cada posible entrada, a cada posible “caso””¹¹⁶, lo que restringe su aplicación a los casos que no se hayan escrito en su

¹¹¹ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a...", *cit.*, p. 15.

¹¹² WEBER, R.H. (2018). ““Rose is a rose is a rose...””, *cit.*, p. 705.

¹¹³ LESSIG, L. (2009). *El código 2...*, *Op. Cit.*, p. 511.

¹¹⁴ HILDEBRANDT, M. (2019). *Law for Computer Scientists...*, *Op. Cit.*, pp. 10-11.

¹¹⁵ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a...", *cit.*, p. 18.

¹¹⁶ GRIMMELMANN, J. (2005). "Regulation by Software", *The Yale Law Journal*, p. 1733. Disponible en: <https://papers.ssrn.com/abstract=2358693> (fecha de consulta 1 de noviembre de 2019).

programación, dejando sin margen de discreción a las personas, pues estas no pueden elegir qué acción tomar.

v. *Más vigilancia y regulación.* La experiencia de internet demuestra que el código se puede modificar y utilizar para satisfacer los intereses de los gobiernos y de las grandes empresas. Internet significó más instrumentos de control, ya que se facilitó el rastreo de las conductas en la red. No olvidemos que todas las anotaciones que se hacen en una cadena de bloques son públicas y, por lo tanto, rastreables. Esto podría ayudar a los regímenes totalitarios a extender y concentrar su poder¹¹⁷.

2. Beneficios del código como ley

La implementación del código como ley también presenta ciertos beneficios, veamos:

i. *Ahorro de costos.* Las cadenas de bloques se rigen por un código técnico, que se puede producir con solo una computadora y se puede distribuir a través de cualquier tipo de dispositivo de almacenamiento o red de conexión¹¹⁸, una ventaja de esto, es que se reducen los costos de cumplimiento legal. Sin embargo, ello no necesariamente siempre es así, porque en las cadenas de bloques de Criptomonedas que utilizan sistemas de minería de prueba de trabajo, tienen un consumo de gasto energético significativo.

ii. *Cumplimiento automático.* El código garantiza el cumplimiento de forma *ex ante*, evitando la infracción antes de que ocurra, disminuyendo finalmente la necesidad de supervisión¹¹⁹ y la intervención terceros (jueces) que juzguen o sancionen la infracción. En lugar de establecer qué conductas están prohibidas o permitidas, como en el caso de las leyes tradicionales, el código restringe o permite lo que los individuos pueden hacer.

¹¹⁷ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 203.

¹¹⁸ DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a..." , cit., p. 5

¹¹⁹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 195.

iii. *Ausencia de reglas ambiguas*. Si bien incluimos esta característica como un riesgo, representa también un beneficio, pues el carácter determinista del código no da cabida a la ambigüedad, excluyendo la necesidad de arbitraje judicial¹²⁰.

3. ¿La nueva *lex mercatoria*? - *lex criptografía*

La *lex Mercatoria* tiene sus orígenes en la alta edad media, como respuesta al rechazo del derecho de los señores feudales¹²¹. Surge en las llamadas ferias “como ordenamiento para regir las relaciones entre los comerciantes de modo uniforme, a través de la aplicación obligatoria de los usos y costumbres comerciales”¹²², estos usos y costumbres habían sido creados por los mismos mercaderes y era la ley aplicable para resolver las disputas en los tribunales comerciales (contaban con sus propios jueces), en vez de las leyes del lugar de procedencia de las partes.

Los comerciantes desarrollaron un sistema en el cual los instrumentos de crédito o préstamos eran representados en pedazos de papel. Con el pasar del tiempo, la *lex mercatoria* fue adoptada por los sistemas jurídicos de todo Europa¹²³. Con la llegada de la tecnología Blockchain y los sistemas de resolución de disputas (creados desde el entorno de la propia tecnología¹²⁴), ha surgido la cuestión de si estaríamos frente al caso de una nueva *lex mercatoria*, en este caso, una *lex criptografía*, en el cual los sistemas jurídicos tradicionales sean desplazados por Blockchain o si, por el contrario, sea esta tecnología la que deba adaptarse a la ley.

¹²⁰ HASSAN, S. & DE FILIPPI, P. (2017). "The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code", *Field Actions Science Reports: The Journal of Field Actions*, Vol. Special Issue 17, p. 89. Disponible en: <https://papers.ssrn.com/abstract=3117630> (fecha de consulta: 31 de agosto de 2019).

¹²¹ LEON-ROBAYO, E. (2019). *La nueva lex Mercatoria en el derecho latinoamericano de contratos*, Tirant lo Blanch - Universidad del Rosario, Bogotá, Colombia, p. 31.

¹²² PÉREZ CÁZARES, M. E. (2018). “La *lex mercatoria* una ley procesal global”, *Derecho global. Estudios sobre derecho y justicia*, Vol., 3, No. 9. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362018000200104 (fecha de consulta: 2 de diciembre de 2022).

¹²³ SCHUSTER, E. (2019). “Cloud Crypto Land”, *LSE Law, Society and Economy*, documento de trabajo No. 17, p. 21. Disponible en: <https://ssrn.com/abstract=3476678> (fecha de consulta: 17 de junio de 2020).

¹²⁴ Véase capítulo IV de la presente obra donde se aborda con más detalle dichos sistemas de resolución de disputas descentralizadas.

La llamada *lex criptografía* estaría conformada por los contratos inteligentes, que son empleados para regular relaciones entre dos o más personas¹²⁵, dado que al codificar un acuerdo legal en un Smart Contracts los contratantes están creando una especie de ley. Al respecto advierte WRIGHT Y otros que con *lex criptografía* “Las personas podrían unirse y establecer reglas para su propio gobierno, recaudar impuestos y distribuir la riqueza de la forma que el grupo considere justa. Las comunidades podrían convertirse en naciones, sin límites geográficos, y ser gobernadas a través de un conjunto de reglas algorítmicas que pueden establecerse mediante mecanismos de votación y Smart Contracts”¹²⁶.

No obstante, es importante mencionar que *lex mercatoria* nunca tuvo una adopción y aceptación completa por parte de los sistemas jurídicos europeos, pues, como explica SCHUSTER, aunque el desarrollo de los instrumentos negociables fue una forma eficiente de resolver un problema para la que no había soluciones sencillas (debido a las grandes distancias, no había forma de comunicación segura entre los comerciantes), e hizo posible un comercio internacional (que se tradujo en beneficios para los Estados y para el ordenamiento jurídico), que no hubiese tenido lugar sin *lex mercatoria*. Estos instrumentos negociables, siempre estuvieron sometidos a la ley de cada estado, como, por ejemplo, si la firma de un cheque fuese falsa, esto haría que el título fuese nulo¹²⁷.

En este sentido, vemos demasiado optimista pensar que la tecnología Blockchain reemplazará a los sistemas legales tradicionales, primero, porque no ofrece mejores alternativas que el derecho tradicional, en ese marco, es solo una herramienta que puede brindar eficiencia para automatizar ciertas tareas. Segundo, porque como tendremos oportunidad de ver más adelante, el código no es infalible, ni tampoco perfecto, por lo que siempre será necesario la intervención del derecho para solucionar circunstancias no previstas o indeseables¹²⁸ y, por último, pero no menos importante, porque Blockchain es

¹²⁵ BECKER, K. (2022). “Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries”, *Law and Critique*, Vol. 33, No. 2, p. 118. Disponible en: <https://link.springer.com/article/10.1007/s10978-021-09317-8> (fecha de consulta: 23 de junio de 2022).

¹²⁶ WRIGHT, A. & DE FILIPPI, P. (2015). “Decentralized Blockchain Technology and the Rise of Lex Cryptographia”, p. 39. Disponible en: <https://papers.ssrn.com/abstract=2580664> (fecha de consulta 16 de abril de 2019).

¹²⁷ SCHUSTER, E. (2019). “Cloud Crypto Land”, *cit.*, pp. 21-22.

¹²⁸ LOPEZ-RODRIGUEZ, A. (2021). “Applicable Law to Smart Contracts and Lex Cryptographia”, *Cuadernos Derecho Transnacional*, Vol. 13, No. 1, p. 450. Disponible en: <https://e-revistas.uc3m.es/index.php/CDT/article/view/5966> (fecha de consulta: 2 de diciembre de 2022).

una tecnología que actualmente está siendo regulada, los reguladores, aunque a paso lento, están comprendiendo cómo funciona, sus limitaciones y capacidades; de tal manera, que no hay razones para pensar que esta desplace a la ley tradicional.

El Estado de derecho no es tan ineficientes para que deban ser reemplazado por un gobierno del código informático. No es deseable que el código regule y controle cada aspecto de nuestras vidas, pues podría conducir a una versión moderna de un régimen totalitario, que ordenan a las personas lo que pueden o no hacer, sin ningún tipo de garantías constitucionales o base democrática¹²⁹. Esto solo sucedería si permitimos que los programadores definan nuestro futuro.

3.1 Desafíos regulatorios de la tecnología Blockchain

Si bien, como hemos mencionado anteriormente, la naturaleza autónoma, distribuida y ubicua de las cadenas de bloques públicas hace que sea complejo para los gobiernos regular y controlar la red de nodos. Estas necesitan de la presencia de varios intermediarios para mantenerlas¹³⁰. A pesar de parecer que son sistemas cerrados y que debido a sus características se dificultan los objetivos regulatorios, una Blockchain depende de mineros, fabricantes de *hardware*, desarrolladores de *software*, quienes actúan como un punto de comunicación con el mundo real, pues estos “operan en una jurisdicción particular y, por lo tanto, pueden ser regulados por los gobiernos locales, estatales o nacionales”. Estos intermediarios son y serán los objetivos de la intervención reguladora¹³¹.

Otra de las razones que hacen que Blockchain sea una tecnología difícil de regular es que las partes permanecen anónimas (o más bien seudónimas). No obstante, la arquitectura de las cadenas de bloques es transparente, así que las anotaciones que se hacen en el libro mayor distribuido son públicas y pueden ser rastreadas con minería de datos y programas informáticos, esta característica facilita la identificación de los usuarios, por lo que podría cambiar su falta de regulación.

¹²⁹ WRIGHT, A. & DE FILIPPI, P. (2015). "Decentralized Blockchain...", *cit.*, p. 43.

¹³⁰ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 173

¹³¹ Tal y como lo indica en la doctrina, YEUNG, K. (2019) "Regulation by Blockchain...", *cit.*, p. 219.

Si bien pareciera que las aplicaciones basadas en Blockchain obstaculizan la aplicación legal, la relación entre Blockchain y la ley no debería ser hostil. Es más, incluso podría y debería ser de apoyo y complemento¹³². A continuación, abordaremos las formas de regulación de las cadenas de bloques.

3.2 Cómo regular: formas de abordar la regulación

A la hora de analizar la regulación de internet, LAWRENCE LESSIG planteó en el código y otras leyes del ciberespacio la teoría del pobre punto o las cuatro modalidades de regulación, en la cual el comportamiento humano está regulado por una compleja interrelación de 4 fuerzas diferentes y complementarias, que son, las leyes, las normas sociales, los mercados y la arquitectura física¹³³.

i. Las leyes son la modalidad más directa en la que los gobiernos pueden restringir determinado comportamiento bajo el amparo de que, en caso de incumplimiento, habrá una sanción.

ii. Pero las leyes solo son una forma de regulación, las normas sociales también limitan el comportamiento de un individuo¹³⁴, ejerciendo restricciones y limitando la conducta. Por ejemplo, si una persona desea fumar en el interior de un coche, a pesar de que no esté prohibido por la ley, es probable que solicite permiso al resto de pasajeros¹³⁵. Piense también, por ejemplo, hablar en una red social acerca de tener una postura moralmente inaceptable sobre un tema socialmente relevante y notará el repudio de los demás miembros.

iii. El mercado “también impone su restricción”¹³⁶ y a diferencia de las leyes y las normas sociales, no amenaza y recrimina el comportamiento¹³⁷. Por ejemplo, piense visualizar un video en una plataforma como YouTube y verá cómo estará

¹³² YEUNG, K. (2019) "Regulation by Blockchain...", *cit.*, p. 210.

¹³³ LESSIG, L. (2001). *El código y otras ...*, Op. Cit., p. 204.

¹³⁴ GRIMMELMANN, J. (2005). "Regulation by ...", *cit.*, p. 1724.

¹³⁵ LESSIG, L. (2001). *El código y otras ...*, Op. Cit., p. 205.

¹³⁶ LESSIG, L. (2001). *El código y otras ...*, Op. Cit., p. 205.

¹³⁷ GRIMMELMANN, J. (2005). "Regulation by ...", *cit.*, p. 1725.

cargada de anuncios su reproducción, o si intenta acceder a plataformas de películas en streaming tendrá que pagar un precio para poder visualizarlo.

iv. La última modalidad de regulación la constituye la arquitectura física, que a diferencia de las modalidades anteriores es más difícil de incumplir. La arquitectura de internet son el *software* y el *hardware*, y constituyen un conjunto de restricciones sobre el modo en que las personas se pueden comportar en él. Restringe del mismo modo en que lo hace la arquitectura en el espacio real¹³⁸, como, por ejemplo, los reductores de velocidad obligan a desacelerar.

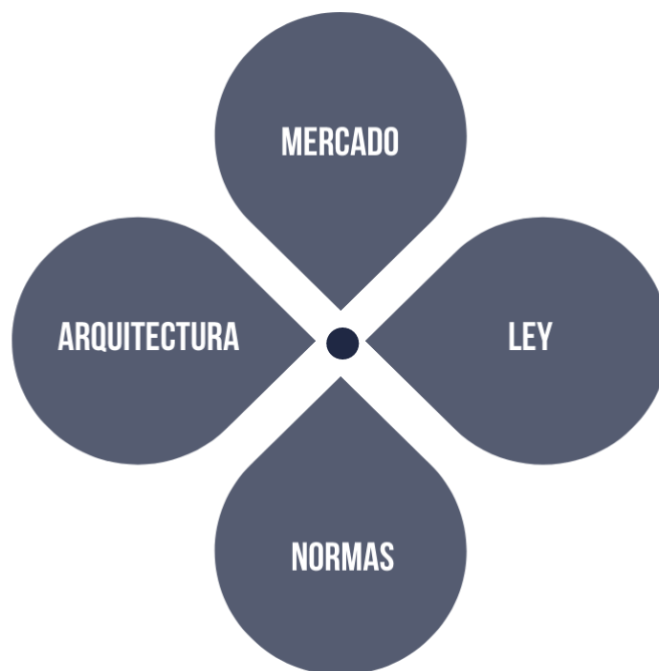


Figura No. 1. La teoría del pobre punto de Lessig o las 4 modalidades de regulación de un individuo. Adaptado de LESSIG, L. (2001). *El código y otras ...*, Op. Cit., p. 218.

En 2018 DE FILIPPI y WRIGHT se plantearon si era posible aplicar esta teoría de regulación a Blockchain, teniendo en cuenta que es una tecnología basada en códigos que operan de forma distribuida e independientemente de cualquier persona física o jurídica¹³⁹. Argumentan que pareciera que, en principio los gobiernos podrían perder “la capacidad de controlar las redes basadas en Blockchain”, pero que ello es una idea

¹³⁸ LESSIG, L. (2001). *El código y otras ...*, Op. Cit., p. 209

¹³⁹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 174.

engañosa debido a que las cadenas de bloques, al igual que internet, son una red descentralizada, y que incluso los sistemas autónomos están sujetos a ciertas restricciones. Continúan señalando que, de hecho, las redes Blockchain necesitan de intermediarios y que estos a su vez son susceptibles de regulación. Además, la arquitectura de Blockchain, es decir, su *software* y *hardware*, dependen de las dinámicas del mercado y están sujetas a las normas sociales¹⁴⁰.

En este sentido, la experiencia reguladora de internet, debería de servir como punto de partida para regular Blockchain. Como se ha mencionado, esta es una tecnología que se puede regular, incluso es probable que se adapte a algunas leyes existentes, por ejemplo, en materia contractual, no obstante, ello no significa que sea fácil y que tal adaptación no conlleve a ciertos desafíos dadas sus características únicas.

¹⁴⁰ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 175.

CAPÍTULO DOS

BLOCKCHAIN Y LOS CONTRATOS INTELIGENTES

CAPITULO DOS: BLOCKCHAIN Y LOS CONTRATOS INTELIGENTES

I. LOS CONTRATOS INTELIGENTES

1. Introducción

Los contratos inteligentes representan una de las innovaciones más interesantes y disruptivas que ha traído consigo el desarrollo de la tecnología Blockchain, aunque como tendremos oportunidad de ver, su conceptualización es previa a la aparición de dicha tecnología. Sus defensores argumentan que la capacidad que tienen los Smart Contracts de automatizar las cláusulas y el cumplimiento de las obligaciones, los hace más eficiente que sus homólogos de papel. Incluso, se ha llegado afirmar que reemplazaran a los sistemas clásicos de contratación. No obstante, a pesar de todo el bombo que se les ha dado, muchas veces exagerado por la novedad, este tipo de contratación presenta una serie de desafíos legales, sociales y técnicos para su implementación, los cuales serán objeto de estudio del presente capítulo. Creemos que la implementación y adopción de este tipo de contratación se hará de forma más moderada y limitada.

Nos proponemos, a modo de introducción, analizar los orígenes de este tipo de contratación, luego, discutimos si constituyen o no acuerdos válidos de acuerdo a la legislación española. Posteriormente, analizamos los diferentes tipos de contratos inteligentes y los límites técnico/legales a los que se enfrentan, para luego explorar cómo deberían ser los Smart Contracts para superar los desafíos derivados de la inmutabilidad e inflexibilidad del código. A continuación, examinamos la problemática que subyace de la autoejecución del código y las implicaciones en caso de que haya errores de programación. Asimismo, se analiza su concepto, características, desarrollo y funcionamiento en una Blockchain. Finalmente, el capítulo aborda las fallas que se presentan al traducir un contrato escrito en lenguaje natural al código informático y se expone la importancia de la ambigüedad y la flexibilidad como características deseables en los procesos de contratación tradicional. Finalizamos concluyendo que, quizás, las versiones exitosas que veamos de los contratos inteligentes requieran de un acuerdo en papel de respaldo, dado que, hay obligaciones que dependen del comportamiento humano y, por lo tanto, no son susceptibles de representación en el código.

2. El ascenso de los Smart Contracts

Si bien, en los últimos años hemos observado que los acuerdos de ejecución automática (o plasmados en el código) han ganado bastante popularidad y entusiasmo gracias a la irrupción de las criptomonedas, lo cierto es que su uso y concepto es previo al surgimiento de las cadenas de bloques¹⁴¹ e incluso al del internet y la explosión del comercio electrónico¹⁴².

Su origen se halla en 1948, sobre el puente aéreo de Berlín, debido al caos que le generaba al ejército de Estados Unidos coordinar la logística de las toneladas de provisiones que llegaban para alimentar a la República Federal de Alemania. El sistema de papel era muy lento así que, para solucionar este inconveniente, el sargento mayor del ejército, ED GUILBERT, desarrolló un manifiesto electrónico estándar que podría transmitirse por telex, telégrafo y teléfono¹⁴³. Casi dos décadas más tarde, en 1965, trabajando para la compañía DuPont, mejoraría dichos manifiestos y nacería el sistema de Intercambio Electrónico de Datos (EDI, por sus siglas en inglés). EDI consiste en un estándar GS1¹⁴⁴ y se define como “el intercambio de datos de en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o administrativas”¹⁴⁵.

Este sistema ha venido siendo utilizado por empresas durante varias décadas para comunicarse electrónicamente (de ordenador a ordenador) a través de las cadenas de

¹⁴¹ “BankThink Smart Contracts Were Around Long Before Cryptocurrency”. (2016). Disponible en: <https://www.americanbanker.com/opinion/smart-contracts-were-around-long-before-cryptocurrency> (fecha de consulta: 17 de junio de 2020).

¹⁴² PARDOLESI, R. & DAVOLA, A. (2019). “What is wrong in the debate about smart contracts working paper”, p. 7. Disponible en: <https://ssrn.com/abstract=3339421> (fecha de consulta: 16 de agosto de 2019). A pesar de que no necesiten una Blockchain para existir, hay programadores como DIEHL, S.T. (Sin fecha) “The Handwavy Technobabble Nothingburger” Disponible en: <https://www.stephendiehl.com/blog/nothing-burger.html> (fecha de consulta: 1 de noviembre de 2021) que han advertido que, “sin una cadena de bloques se vuelven demasiado de frágiles, inseguros o estrictamente inferiores a una alternativa centralizada”

¹⁴³ HAYES, F. (2002). “The Story So Far”. Disponible en: <https://www.computerworld.com/article/2576616/the-story-so-far.html> (fecha de consulta: 16 de junio de 2020).

¹⁴⁴ La ASOCIACIÓN DE FABRICANTES Y DISTRIBUIDORES. (Sin fecha). “¿Qué es el estándar GS1?”. Disponible en: <https://www.aecoc.es/generador-codigo-barras/#FAQS> (fecha de consulta: 17 de junio de 2020) define que el Estándar GS1 “es un lenguaje común a nivel global que permite: Identificar información mediante códigos estructurados de forma única y no ambigua: productos, servicios, envíos, empresas; capturar la información con símbolos gráficos definidos y compartirlos datos utilizando sistemas de comunicación estandarizados.”

¹⁴⁵ PESO NAVARRO, E. (1966). “Resolución de conflictos en el intercambio electrónico de documentos” *Cuadernos de derecho judicial*, No. 11, p. 199, como se citó en MORENO, M. (1999). *Contratos electrónicos*, Marcial Pons, Madrid, p. 15.

suministros y redes entre empresas, (a partir de ahora nos referiremos a este tipo de relaciones contractuales como B2B)¹⁴⁶. Las compañías habitualmente lo usan para facturas, intercambio de órdenes de compra, solicitudes de préstamo, inventarios, conocimientos de embarque, entre otros. Este sistema elimina la necesidad del uso del papel y automatiza la información, permitiendo compartirla de forma rápida¹⁴⁷ y eficiente, sin embargo, no hace posible intercambiar pagos y dinero ¹⁴⁸.

En sus primeros días, el Intercambio Electrónico de Datos generó una ola de entusiasmo pues se le veía como sustituto de los contratos de papel. No obstante, a pesar de que redujo algunos costos de transacción ¹⁴⁹, no logró reemplazar la forma en que se suscriben las obligaciones comerciales¹⁵⁰, pues, prestó poca atención a “las necesidades y obligaciones contractuales de las partes”¹⁵¹. En este sentido, advierten GOVERNATORI y otros¹⁵² que, “estos estándares se centraron en las estructuras y protocolos de mensajes en apoyo de las transacciones comerciales. Abordaron solo un número limitado de posibles transacciones contractuales, lo que resultó en una expresividad limitada en comparación con las posibilidades que ofrecen hoy los contratos inteligentes”.

Aunque este sistema logró computarizar las cláusulas de un acuerdo, el criptógrafo NICK SZABO, observó las limitaciones y concluyó que no se aprovechaban los protocolos de cifrados y algoritmos que le otorgaran seguridad e “inteligencia” a las transacciones, quedando los contratos como simples reafirmaciones de los términos y

¹⁴⁶ WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *Duke law journal*, Vol. 67, No. 2, p. 108. Disponible en: <https://ssrn.com/abstract=2936294> (fecha de consulta: 20 de agosto de 2019).

¹⁴⁷ IBM. (Sin fecha). “Intercambio electrónico de datos (EDI)”. Disponible en: <https://www.ibm.com/es-es/supply-chain/edi-electronic-data-interchange> (fecha de consulta: 20 de junio de 2020).

¹⁴⁸ TAPSCOTT, D. & TAPSCOTT, A. (2017). *La revolución blockchain*, 4. Edición, Deusto, Barcelona, p. 105.

¹⁴⁹ SKLAROFF, J. (2017). "Smart Contracts and the Cost of Inflexibility", *University of Pennsylvania Law Review*, Vol. 166, No. 1, p. 263. Disponible en: <https://ssrn.com/abstract=3008899> (fecha de consulta: 1 de abril de 2020).

¹⁵⁰ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 73.

¹⁵¹ SZABO, N. (1996). “Smart Contracts: Building Blocks for Digital Markets”. Disponible en: <https://medium.com/astec/contratos-inteligentes-bloques-de-construcci%C3%B3n-para-mercados-digitales-8d5bd273a462> (fecha de consulta: 16 de abril de 2020).

¹⁵² GOVERNATORI, G., IDELBERGER, F., MILOSEVIC, Z., RIVERET, R., SARTOR, G. & XU, X. (2018). "On legal contracts, imperative and declarative smart contracts, and blockchain systems", *Artificial Intelligence and Law*, Vol. 26, No. 4, p. 384. Disponible en: <https://link.springer.com/article/10.1007/s10506-018-9223-3> (fecha de consulta: 28 de noviembre de 2020).

condiciones existentes en formato tradicional, solo que con algunas modificaciones para el entorno electrónico¹⁵³.

Como resultado, el criptógrafo ideó una “nueva forma de ejecutar contratos electrónicos”¹⁵⁴, que permitiese superar estas limitaciones y lograr un cambio de paradigma en los contratos tradicionales. Así fue, como por primera vez se teorizó¹⁵⁵ el concepto de contratos inteligentes.

NICK SZABO, introdujo el concepto de los contratos inteligentes en un documento de 1994 titulado como, “*Smart Contracts*”, y más tarde lo perfeccionaría, en una serie de artículos publicados a lo largo la década de los noventas. En este documento, exiguamente describía un Smart Contracts como un “algoritmo de transacción computarizado que ejecuta los términos de un contrato”¹⁵⁶. El ejemplo típico y primitivo de Smart Contracts que ejemplarizó¹⁵⁷, fue la humilde máquina expendedora, ya que una vez que la máquina recibe el dinero, esta cumple automáticamente con la entrega del producto y el cambio.

Luego lo definiría como, “un conjunto de promesas, especificadas en forma digital, incluidos los protocolos dentro de los cuales las partes cumplen estas promesas”¹⁵⁸. En otro artículo publicado en 1997 titulado como, “*Formalizing and Securing Relationships on Public Networks*”, señaló que los protocolos criptográficos podrían permitir escribir cláusulas contractuales que crearan relaciones jurídicas seguras y evitan el comportamiento oportunista.

¹⁵³ SZABO, N. (1997). “Formalizing and Securing Relationships on Public Networks”, *First Monday*, Vol. 2, No.9. Disponible en: <https://doi.org/10.5210/fm.v2i9.548> (fecha de consulta 1 de abril de 2020).

¹⁵⁴ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 73.

¹⁵⁵ DELL'ERBA, M. (2019). “Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation””, *University of Pennsylvania Journal of Law & Public Affairs*, p. 12. Disponible en: <https://ssrn.com/abstract=3228445> (fecha de consulta: 2 de agosto de 2019).

¹⁵⁶ SZABO, N. (1994). “Smart Contracts”. Disponible en: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> (fecha de consulta: 16 de abril de 2020). Mas tarde en SZABO, N. (1996). “Smart Contracts...”, *cit.*, lo definiría como un conjunto de promesas, especificadas en forma digital, que incluye los protocolos dentro de los cuales las partes cumplen con estas promesas.

¹⁵⁷ SZABO, N. (1996). “Smart Contracts: Building....”, *cit.*

¹⁵⁸ SZABO, N. (1996). “Smart Contracts...”, *cit.*

No obstante, estas primeras ideas acerca de los Smart Contracts permanecieron aisladas durante muchos años¹⁵⁹, (i) en parte, porque la infraestructura económica y de comunicaciones de los noventa era insuficiente para soportar los protocolos planteados por el criptógrafo¹⁶⁰, (ii) ello unido a la incapacidad del sistema financiero de soportar transacciones automáticas¹⁶¹; ya que las transferencias bancarias se procesaban y aún hoy se procesan por lotes¹⁶².

El desarrollo que hizo que los planteamientos de SZABO pasaran de ser un mero concepto teórico a una realidad práctica fue la tecnología Blockchain¹⁶³. Bitcoin permitió transacciones enteramente digitales y la ejecución limitada de contratos inteligentes¹⁶⁴. Más tarde, progresarían con el lanzamiento de otras cadenas de bloques, como Ethereum, la cual proporcionaría los protocolos necesarios para desarrollar la tecnología propuesta por el criptógrafo¹⁶⁵, y allanar el camino para convertirla en una propuesta comercial viable¹⁶⁶.

¹⁵⁹ WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *cit.*, p. 112.

¹⁶⁰ OMOHUNDRO, S. (2014). "Cryptocurrencies, smart contracts, and artificial intelligence", *AI matters*, Vol. 1, No. 2, p. 19. Disponible en: <https://doi.org/10.1145/2685328.2685334> (fecha de consulta: 16 de agosto de 2020).

¹⁶¹ CASSANO, J. (2014). "What Are Smart Contracts? Cryptocurrency's Killer App". Disponible en: <https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app> (fecha de consulta: 16 de agosto de 2020).

¹⁶² Por ejemplo, en el procesamiento de transacciones financieras de los Estados Unidos (realizado por la red ACH *automated clearing house*, la cual es administrada por la Reserva federal), cuando un usuario quiere enviar dinero a otro usuario, o pagar una factura, debe rellenar un formulario que contiene el monto de la transacción y los datos bancarios del receptor, con esta información se hace una solicitud de pago que se transmite a su banco. Una vez es recibida por el banco del remitente, este hace unas pruebas de seguridad para verificar que el titular autorizó la transacción y que cuenta con los saldos suficiente para realizarla. Con esta información el banco generará un archivo de mensaje de texto estandarizado, que se transmitirá por la red ACH al banco del receptor, luego este identificará el número de cuenta del receptor y le notificará que ha recibido dinero a su cuenta.

Estas comunicaciones no se realizan en tiempo real, ya que sería sumamente prohibitivo (es por esto que realizar una transacción que se reciba el mismo día es costoso), por lo que las transacciones se agrupan por lotes en orden de llegada y se envían en horas determinadas del día. Todas las solicitudes se agrupan en un solo archivo y se remiten todas a la vez a la red ACH.

¹⁶³ WRIGHT, A. & DE FILIPPI, P. (2015). "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". Disponible en: <https://papers.ssrn.com/abstract=2580664> (fecha de consulta 16 de abril de 2019). Véase también WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *cit.*, p. 112.

¹⁶⁴ PEREIRA, J. (2019). "The genesis of the revolution in Contract Law", *ACM*, p. 375. Disponible en: <http://dl.acm.org/citation.cfm?id=3326414> (fecha de consulta: 25 de septiembre de 2020).

¹⁶⁵ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 73. Ver también TUR FAÚNDEZ, C. (2018). *Smart contracts: análisis jurídico*, Ed.: Reus, Madrid, p. 53, GIANCASPRO, M. (2017). "Is a 'smart contract' really a smart idea? Insights from a legal perspective", *Computer Law & Security Review*, Vol. 33, No. 6, p. 825. Disponible en: <http://www.sciencedirect.com/science/article/pii/S026736491730167X> (fecha de consulta: 16 de abril de 2019).

¹⁶⁶ AL KHALIL, F., CECI, M., O'BRIEN, L. & BUTLER, T. (2017). "A Solution for the Problems of Translation and Transparency in Smart Contracts", p. 3. Disponible en: <https://tinyurl.com/y4mdetzk> (fecha de consulta: 6 de octubre de 2020).

II. SMART CONTRACTS Y EL DERECHO CONTRACTUAL

1. Planteamiento

Una parte amplia de la investigación jurídica de los Smart Contract se ha centrado sobre el derecho contractual, específicamente, el debate se ha dirigido hacia la expectativa de que los contratos inteligentes tengan o no la capacidad de redefinir las bases fundamentales de los sistemas clásicos de contratación¹⁶⁷, en sí pueden considerarse contratos a la luz del derecho, o si, por el contrario, solo son un nombre elegante para designar al código de ordenador¹⁶⁸.

Las condiciones que exige la ley para que un acuerdo genere un vínculo jurídico son bastante flexibles. La legislación civil dota a los contratantes de plena autonomía para contratar y solo basta con integrar los elementos esenciales del contrato, (consentimiento, objeto y causa) para que sea legalmente exigible. De tal forma que los acuerdos que se redacten en lenguaje de programación pueden ser considerados como contratos legales, siempre y cuando reúnan tales requisitos.

Sin embargo, los Smart Contracts que se ejecuten en Blockchain suponen un obstáculo a la hora de convertirse en acuerdos válidos según la ley contractual, debido a que, en muchos casos, como no se conoce la identidad de los contratantes, no se estaría prestando un consentimiento válido. ¿Se pueden superar estas limitaciones? O, por el contrario, ¿será necesario una modificación ontológica de los elementos esenciales del contrato?

¹⁶⁷ Véase EUROPEAN LAW INSTITUTE. (2022). *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection Council Draft*. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection_Council_Draft.pdf (fecha de consulta: 12 de agosto de 2022), DELL'ERBA, M. (2019). "Demystifying Technology...", *cit.*, p. 12 y EENMAA-DIMITRIEVA, H. & SCHMIDT-KESSEN, M.J. (2019). "Creating markets in no-trust environments: The law and economics of smart contracts", *Computer Law & Security Review*, Vol. 35, No. 1, pp. 69 y ss. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918303558> (fecha de consulta: 2 de abril de 2019).

¹⁶⁸ GREENSPAN, G. (2016). "Beware of the Impossible Smart Contract". Disponible en: <https://www.the-blockchain.com> como se citó en PARDOLESI, R. & DAVOLA, A. (2019). "What is wrong in ...", *cit.*, p. 1, véase TAKAHASHI, K. (2018). "Blockchain and Smart Contract for Contract Management (Dispute Prevention and Generation)", p. 5. Disponible en: SSRN: <https://ssrn.com/abstract=3566678> (fecha de consulta: 17 de mayo de 2020).

Algunos podrían argumentar que se podría superar con un cambio en la arquitectura de las cadenas de bloques públicas en el que se solicite la identificación de las partes, sin embargo, es un cambio de diseño que en principio iría en contra de las bases ideológicas de la tecnología, pero supondría la adecuación de los contratos inteligentes al cuerpo normativo existente.

En esta sección trataremos de abordar estos asuntos y brindar una visión crítica y amplia, primero analizaremos si los Smart Contracts cumplen con los requisitos esenciales, luego procederemos a analizar si cada tipo de contrato inteligente cumple o no con dichos elementos, habida cuenta de que no es dable generalizar y afirmar que todos los contratos inteligentes no cumplen plenamente con estos requisitos. Por ello, haremos un análisis por separado de los mismos, pues cada cual cuenta no solo con limitaciones legales, sino también con limitaciones técnicas.

2. El contrato inteligente como contrato legal

Probablemente, la discusión de si se puede considerar el código del contrato inteligente como un contrato legal o no, es una de las cuestiones que más se han abordado por la literatura jurídica en lo relacionado con esta tecnología. En consecuencia, el análisis de estas preocupaciones es amplio y heterogéneo. Para algunos, los contratos inteligentes no se pueden considerar contratos¹⁶⁹ y, para otros, como JIMÉNEZ LINARES, encajan perfectamente en lo que para el derecho puede considerarse como contrato¹⁷⁰, siempre y cuando estos cumplan con los requisitos esenciales para la formación de los contratos.

¹⁶⁹ O'SHIELDS, R. (2017). "Smart Contracts: Legal Agreements for the Blockchain", *North Carolina Banking Institute*, Vol. 21, No. 1, p. 185. Disponible en: <https://scholarship.law.unc.edu/ncbi/vol21/iss1/11/> (fecha de consulta: 1 de diciembre de 2019).

¹⁷⁰ Véase JIMÉNEZ LINARES, M. (2020). "De los contratos inteligentes (Smart Contracts) a los contratos legales inteligentes: problemática técnico-jurídica. El contrato Blockchain", *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (Dir. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra, pp. 325-358, FELIÚ, R. (2018). "Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado", *La Ley Mercantil*, No. 47. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247775 (fecha de consulta: 23 de septiembre de 2021), DUROVIC, M., & JANSSEN, A. (2019). "The Formation of Blockchain-based Smart Contracts in the Light of Contract Law", *European Review of Private Law*, pp. 753-772. Disponible en: <http://static.ie.edu.s3.amazonaws.com/Tertulia/Papers%202018/Papers/The%20Formation%20of%20Blockchain-based%20Smart%20Contracts%20in%20the.pdf> (fecha de consulta: 23 de septiembre de 2021), EUROPEAN LAW INSTITUTE. (2022). *ELI Principles...*, Op. Cit., p. 35, LEGERÉN-MOLINA, A. (2018). "Los contratos inteligentes en España (La disciplina de los smart contracts) / Smart contracts in Spain; the regulation of smart contracts", *Revista De Derecho Civil*, Vol. 5, No. 2, p. 220. Disponible en: <https://www.nreg.es/ojs/index.php/RDC/article/view/320> (fecha de consulta: 14 de abril de 2020), DELL'ERBA, M. (2019). "Demystifying Technology...", cit., p. 24, WERBACH, K. & CORNELL, N. (2017) y "Contracts ex machina", cit., p. 339.

Los contratos legales inteligentes que se ejecutan en Blockchain, suponen un desafío para el derecho contractual tradicional, dada su naturaleza distribuida, seudónima, descentralizada e inmutable. Ahora bien, pero, ¿pueden los contratos inteligentes ser exigibles legalmente y, por tanto, tener efectos vinculantes para las partes en la legislación española?

En principio, la respuesta depende del tipo de contrato inteligente. Conforme a lo recogido en el código Civil¹⁷¹, los contratos serán obligatorios, sin importar la forma en la que se hayan celebrado, siempre y cuando concurran las condiciones esenciales para su validez. De igual forma, el artículo 23.3 de la Ley de Servicios de la sociedad de la información y de comercio electrónico (LSSICE) señala que, “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”¹⁷². En este sentido, el contrato inteligente es, como señala BARCELÓ¹⁷³, una forma de contrato electrónico, regulado por LSSICE. Por tanto, cualquiera que sea la manera en que se exprese un acuerdo, ya sea, por ejemplo, verbal, una conversación por chat o una servilleta; puede convertirse en un contrato legalmente exigible, si cumple con las condiciones necesarias para su validez. Luego, entonces, un contrato escrito en código de ordenador, de acuerdo al principio de libertad de forma, puede ser un contrato legalmente exigible. Aun así, ¿puede un Smart contract cumplir con los requisitos esenciales de un contrato? Nos proponemos, pues, analizar, de acuerdo a lo establecido en el código civil español¹⁷⁴, un contrato se constituye válidamente si concurren tres requisitos: consentimiento, objeto y causa de la obligación. Sin estos tres requisitos un

¹⁷¹ España. Real Decreto de 24 de julio de 1889, por el que se publica el Código Civil. *Boletín Oficial del Estado*, 16 de agosto de 1889. Artículo 1278 “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.” Hay que tener en cuenta que la legislación española prevé que para que ciertos contratos sean válidos necesitan estar dotados de una solemnidad, en los que la legislación exige una forma específica para que sean válidos y exigibles, tal y como lo recoge el artículo 1279 “Si la ley exigiere el otorgamiento de escritura u otra forma especial para hacer efectivas las obligaciones propias de un contrato, los contratantes podrán compelerse recíprocamente a llenar aquella forma desde que hubiese intervenido el consentimiento y demás requisitos necesarios para su validez”.

¹⁷² España. Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, *Boletín Oficial del Estado*, 11 de julio de 2002.

¹⁷³ BARCELÓ, R. (2021). “El impacto de la tecnología blockchain en la contratación privada: ¿hacia una contratación inteligente?”, *Revista de los Estudios de Derecho y Ciencia Política*, No. 33, p. 4. Disponible en: <https://raco.cat/index.php/IDP/article/view/n33-barcelo/481692> (fecha de consulta: 17 de enero de 2023).

¹⁷⁴ 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.

contrato no puede existir. Es importante mencionar, dicho sea de paso, que además los Smart Contracts deben cumplir con los requisitos del artículo 23 de la LSSICE.

2.1 Consentimiento

El consentimiento contractual es, como advierte DOMÍNGUEZ GALLEGO, el alma del contrato¹⁷⁵, “es el acuerdo de voluntades de dos a o más personas sobre el objeto y la causa del contrato”¹⁷⁶. Este requisito hace referencia a la capacidad legal de las partes para contratar. El artículo 1263 del código civil español especifica que los sujetos que no pueden prestar consentimiento,¹⁷⁷ preceptuando que todo adulto es capaz, salvo que un juez declare lo contrario. Este elemento es la base para que todo contrato tenga validez y eficacia, en este sentido advierte DÍEZ-PICAZO que, “no se trata de que el consentimiento pueda o no pueda ser prestado, sino del negocio jurídico generado por este consentimiento es o no es un negocio jurídico válido y eficaz. La capacidad no es un presupuesto de la existencia del consentimiento, sino un presupuesto de la validez y eficacia del negocio. Por ello, más que de capacidad para prestar el consentimiento, debe hablarse pura y simplemente de capacidad para contratar”¹⁷⁸.

Según APARICIO, una pieza fundamental del consentimiento es la identidad de las partes, ya que, si estas no pueden ser identificadas, no puede existir un consentimiento válido¹⁷⁹. Esta característica supone un problema para los Smart Contracts que se escriben, se desarrollan y ejecutan íntegramente dentro de una cadena de bloques pública,

¹⁷⁵ DOMÍNGUEZ-GALLEGOS, I. (2021). “Los elementos esenciales del contrato”, *Manual de derecho civil. Vol. 2, Obligaciones y contratos, Teoría general* (Dir. LLAMAS-POMBO, E.), Ed.: Wolters Kluwer, Las Rozas Madrid, p. 280.

¹⁷⁶ MARIN-LOPEZ, M. (2020). “Requisitos esenciales del contrato. Elementos accidentales del contrato”, *Tratado de Contratos*, (Dir. BERCOVITZ, R., MORALESJO N. & QUICIOS), Ed.: Tirant lo Blanch, p. 668.

¹⁷⁷ Art. 1.263. No pueden prestar consentimiento: 1.º Los menores no emancipados, salvo en aquellos contratos que las leyes les permitan realizar por sí mismos o con asistencia de sus representantes, y los relativos a bienes y servicios de la vida corriente propios de su edad de conformidad con los usos sociales. 2.º Los que tienen su capacidad modificada judicialmente, en los términos señalados por la resolución judicial.

¹⁷⁸ DÍEZ-PICAZO, I (2012). *Fundamentos del derecho civil patrimonial I introducción: teoría del contrato*, Thomson Civitas, Madrid, p. 169.

¹⁷⁹ Tal y como advierten, en la doctrina, APARICIO, B. (2018). “Chapter 1: the challenges associated with smart contracts: formation, modification, and enforcement”, *Smart contracts: Is the Law Ready?* (Dir. Smart Contracts Alliance & Chamber of Digital Commerce), p.19. De igual forma LÓPEZ BERENGUER, J. (1950). “La identificación de las personas en la relación jurídica civil”, *Anales de la Universidad de Murcia*, P. 370. Disponible en: <https://tinyurl.com/ycrdful2> (fecha de consulta 15 de mayo de 2020) afirma que, “En general, la identidad de los contratantes viene exigida para todos los contratos, implícitamente, en el apartado 1.º del art. 1.261, según el cual, no hay contrato sino cuando existe «consentimiento de los contratantes»; indudablemente falta ese consentimiento cuando quien lo expresa no es la persona que deba prestarlo”.

porque las partes por lo general pueden permanecer seudónimas, es decir, que tal y como señala LEGERÉN la capacidad exigida a las partes para contratar se dificulta por el carácter anónimo de la tecnología Blockchain¹⁸⁰. Por ejemplo, Ethereum, no comprueba la capacidad legal de sus participantes, por lo que, cualquiera puede acceder a la misma y suscribir contratos, sin importar si es un incapaz, lógicamente esto acarrea consecuencias jurídicas en cuanto a la validez del negocio jurídico¹⁸¹.

Este problema no se presentaría en las Blockchain de carácter privado, ya que estas, al funcionar con controles de acceso para las partes que desean unirse a la red, necesariamente estas tendrán que ser identificadas. Un ejemplo de estos tipos de Smart Contracts serían los de Corda del consorcio R3 que requieren de la identificación de las partes. De tal manera que, en principio, el contrato inteligente que se ejecuta en una cadena de bloques pública no cumple con uno de los requisitos esenciales del contrato, sin embargo, esta afirmación solo es válida, siempre y cuando, las partes no se hayan identificado.

Asimismo, el artículo 1262 del código civil indica que, “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”. Por tanto, dado que una de las partes debe publicar el Smart Contract en la cadena de bloques, es posible que esta publicación pueda ser considerada como una oferta¹⁸². En consecuencia, el consentimiento se producirá cuando la otra parte lo acepta con su clave criptográfica.

2.2 Objeto

El segundo elemento esencial para que haya contrato, es que exista un objeto cierto que sea materia del contrato. “Posiblemente, baste con decir que el objeto del contrato es la realidad social que este ordena o a la que sus pactos conciernen (sea un paquete de acciones, la prestación de un servicio, la solución de una controversia, o la ordenación de las negociaciones), realidad que es susceptible de valorarse

¹⁸⁰ LEGERÉN-MOLINA, A. (2020). “Smart Contracts que se ejecutan en “Blockchain”, *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (Dirs. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra, p. 301.

¹⁸¹ DUROVIC, M., & JANSSEN, A. (2019). “The Formation...”, *cit.*, p. 768.

¹⁸² DUROVIC, M., & JANSSEN, A. (2019). “The Formation...”, *cit.*, p. 762.

económicamente”¹⁸³. Según los artículos 1271 y ss. del código civil¹⁸⁴, debe ser, lícito, posible y determinable.

Lícito, es decir, que no sea contrario a lo establecido en la ley o en las buenas costumbres, como señala MARIN LÓPEZ, “implica la adecuación del objeto al tráfico jurídico de conformidad con el ordenamiento jurídico”¹⁸⁵. Posible, significa que el contrato solo nacerá a la vida jurídica si las prestaciones son posibles, ya que nadie está obligado a lo imposible; y determinable, quiere decir que el objeto debe ser una cosa o servicio identificable al momento de la perfección del contrato.

El lenguaje de programación de un contrato inteligente, técnicamente, puede incorporar las cláusulas que hacen referencia al objeto de un acuerdo, aunque estas tengan que ser de carácter determinista, porque como hemos mencionado anteriormente, no es posible la codificación de ambigüedades. En la legislación española, el código de ordenador es un instrumento válido para definir los derechos y obligaciones de las partes, siempre y cuando si esa sea su intención¹⁸⁶. En este sentido, habrá que analizar cada caso concreto para saber si determinado Smart Contracts cumple o no con este requisito, pues habrá situaciones en las cuales el objeto no sea susceptible de representación en el código.

2.3 Causa

El tercer elemento que ha de reunir todo contrato es la causa¹⁸⁷, que se podría definir como “el fin o resultado perseguido por las partes con la celebración del contrato.

¹⁸³ STS 5 junio 1978, como se citó en 9136 en GARCÍA-VICENTE, J. (2013). “Sección segunda. del objeto de los contratos”, *Comentarios al Código civil* tomo VII (Arts. 1265 a 1484) (DIRS. BERCOVITZ-RODRIGUEZ-CANO, R.), Ed.: Tirant Lo Blanch, Valencia, pp. 9136-9140.

¹⁸⁴ Artículo 1271. 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. No podrán ser objeto de contrato las cosas o servicios imposibles. Artículo 1273. 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.

¹⁸⁵ MARIN-LOPEZ, M. (2020). “Requisitos esenciales...”, *cit.*, p. 737.

¹⁸⁶ APARICIO, B. (2018). “Chapter 1: the challenges associated ...”, *cit.*, p. 19.

¹⁸⁷ Artículo 1274. En los contratos onerosos se entiende por causa, para cada parte contratante, la prestación o promesa de una cosa o servicio por la otra parte; en los remuneratorios, el servicio o beneficio que se remunera, y en los de pura beneficencia, la mera liberalidad del bien hecho. Artículo 1275. Los contratos sin causa, o con causa ilícita, no producen efecto alguno. Es ilícita la causa cuando se opone a las leyes o a la moral. Artículo 1276. La expresión de una causa falsa en los contratos dará lugar a la nulidad, si no se probase que estaban fundados en otra verdadera y lícita. Artículo

Todo contrato ha de tener una causa, y ésta ha de ser lícita y verdadera”¹⁸⁸. Advierte DIEZ PICAZO que el concepto de causa dentro de la teoría del contrato es, de los más oscuros, confusos y difíciles de comprender, para este autor, la causa se configura como el resultado que las partes quieren conseguir, es decir, es el propósito de alcanzar un determinado resultado práctico por medio del contrato¹⁸⁹.

Este elemento no supone ningún obstáculo para la implementación de estos acuerdos. No obstante, la doctrina ha alertado¹⁹⁰ que debido a características como la ejecución automática y a la naturaleza seudónima de las transacciones, podría ser más fácil el despliegue de contratos que permitan actividades ilegales, como ya pasó con la plataforma de mercado negro, Silk Road¹⁹¹. Un contrato inteligente que se considere ilícito se ejecutará si se cumplen las condiciones programadas en su código, sin entrar a valorar la legalidad de tales estipulaciones.

3. Tipos de contratos inteligentes

Teniendo en cuenta que no podemos afirmar de forma categórica que todo Smart contract sea considerado como un contrato legal, puesto que existen una variedad de tipologías de contratos inteligentes que, en algunos supuestos, si se pueden considerar como contratos legales. En este apartado abordaremos los tipos de Smart Contracts y si estos podrían satisfacer los requisitos de formación contractual.

3.1 Contrato escrito y ejecutado íntegramente por el código

Este es un contrato en el cual las cláusulas están representadas y ejecutadas exclusivamente por el código de programación y sin ningún tipo de intervención humana. Como cuestiones generales, genera duda la aplicación de un modelo contractual con estas

1277. Aunque la causa no se exprese en el contrato, se presume que existe y que es lícita mientras el deudor no pruebe lo contrario.

¹⁸⁸MARIN-LOPEZ, M. (2020). “Requisitos esenciales...”, *cit.*, p. 668.

¹⁸⁹DÍEZ-PICAZO, I (2012). *Fundamentos del derecho...*, *Op. cit.*, p. 255 y 275.

¹⁹⁰WRIGHT, A. & DE FILIPPI, P. (2015). "Decentralized Blockchain Technology ...", *cit.*, pp. 41 y ss. Véase también SIMONITE, T. (2015). "Los contratos inteligentes con Bitcoin permitirán distintos tipos de crímenes", *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/5078/los-contratos-inteligentes-con-bitcoin-permitiran-distintos-tipos-de-crime> (fecha de consulta: 26 de marzo de 2019).

¹⁹¹Silk Road fue un sitio negro de comercio electrónico, donde se comercializaba la compra y venta de estupefacientes de forma anónima. En este mercado las transacciones empleaban bitcoin como método de pago y la red Tor para mantener las operaciones en el anonimato. Fue cerrado por el FBI en 2013.

características. Primero, porque la validez legal de un acuerdo, cuya formación, celebración y ejecución está administrada únicamente por el código, en principio no cumpliría con todos los elementos esenciales del contrato, en este caso, el consentimiento. Segundo, porque, aunque el acuerdo sea válido, muchas cláusulas no son susceptibles de automatización, en virtud de que requieren de la intervención humana para su ejecución, interpretación o para la resolución de disputas¹⁹².

De igual forma, la rigidez del código binario implica una serie de costos *ex ante*, dado que las partes deben anticipar con la mayor exactitud posible las contingencias futuras que se puedan presentar, algo que es prácticamente imposible. De hecho, así lo asume el derecho contractual tradicional, que viene a corregir estas fallas de forma *ex post*¹⁹³. Por tanto, ello supone una movilización de recursos, ya que como advierte SKLAROFF, las partes deben aprender más sobre el estado futuro del mundo y, en caso de que sus pronósticos sean insuficientes, pueden verse en la necesidad de presentar una demanda¹⁹⁴ para corregir esas fallas que no fueron previsibles. Es importante destacar, dicho sea de paso, que cada paso de ejecución del contrato debe pagar una tarifa, lo que incrementa los costos que deben asumir las partes para la implementación del mismo.

En consecuencia, se desvela que quizás el discurso generalizado acerca de los beneficios de los Smart Contracts como instrumentos para reducir costos de transacción puede ser un sofisma. Como acertadamente afirma VERSTRAETE, “(...) los contratos inteligentes dependen de su conveniencia normativa de la creencia de que es factible formar acuerdos completos. Empíricamente, este no es el caso. Los contratos están incompletos y el sistema legal proporciona términos implícitos para remediar este problema. En resumen, los costos de formar acuerdos completos probablemente superarían los supuestos beneficios de los contratos inteligentes”¹⁹⁵. Es decir, ello derrota uno de los principales objetivos de esta tecnología.

¹⁹² ADLERSTEIN, D. (2017). “Are Smart Contracts Smart? A Critical Look at Basic Blockchain Questions”. Disponible en: <https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract> (fecha de consulta: 16 de marzo de 2020).

¹⁹³ TJONG TJIN TAI, E. (2019). “Challenges of Smart Contracts”, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, p. 98.

¹⁹⁴ SKLAROFF, J. (2017). “Smart Contracts and the ...”, *cit.*, p. 280.

¹⁹⁵ VERSTRAETE, M. (2019). “The Stakes of Smart Contracts”, *Loyola University Chicago Law Journal*, Vol. 50, p. 789. Disponible en: <https://ssrn.com/abstract=3178393> (fecha de consulta: 3 de febrero de 2020).

Naturalmente, es peligroso que el código controle todo el acuerdo, ya que la plataforma donde se aloja el Smart Contract puede ser víctima de un ataque informático o pueda que el código contenga errores de codificación que necesiten de la intervención humana para su posterior corrección o modificación. En este sentido, es fundamental que existan contingencias que subsanen estas deficiencias. No debemos olvidar lo sucedido con el DAO, administrado únicamente por el código y en cuyos términos y condiciones escritos en lenguaje natural, se informaba que esta información era ofrecida con fines educativos, pero que en ningún caso reemplazaba los términos expresos del código DAO establecido en la cadena de bloque.

Incluso se advertía que cualquier discrepancia del código DAO “*0xbb9bc244d798123fde783fcc1c72d3bb8c189413*”, con dichos términos, primaría el código¹⁹⁶. Precisamente, ese fue el alegato del atacante del DAO, ya que este argumentaba que su acción era legítima, porque la función estaba codificada en el código del contrato inteligente¹⁹⁷. Es relevante anotar que tal y como advierten CIEPLAK y otros, los inversores de la DAO no emprendieron acciones legales porque no se conocían a las partes contra las que se haría cumplir el contrato¹⁹⁸.

De cualquier manera, la aplicación de un acuerdo basado en código no se debería determinar solo por el contenido de este, pese a que la libertad de contratación es bastante flexible, las partes todavía no pueden rechazar a las normas imperativas o de orden público, así que el derecho siempre intervendrá para establecer límites.

Incidentes de este tipo demuestran que por más que los entusiastas tecnolibertarios defiendan que los contratos inteligentes no necesitan del sistema jurídico o de intervención humana para su ejecución, muchas veces este es y será necesario.

¹⁹⁶ Más información en “Explanation of Terms and Disclaimer, The DAO”. (2016). Disponible en: <https://perma.cc/7QV6-HWUT> (fecha de consulta: 18 de diciembre de 2019).

¹⁹⁷ Ver carta escrita por el atacante en “An Open Letter”. (2016). Disponible en: <https://pastebin.com/CcGUBgDG> (fecha de consulta: 18 de diciembre de 2019).

¹⁹⁸ CIEPLAK, J. & LEEFATT, S. (2017). “Smart Contracts: A Smart Way to Automate Performance”, *Georgetown law technology review*, Vol. 1, p. 426. Disponible en: <https://georgetownlawtechreview.org/smart-contracts-a-smart-way-to-automate-performance/GLTR-04-2017/> (fecha de consulta: 9 de abril de 2020).

3.2 Contrato inteligente que tiene un envoltorio en papel

Este es un contrato tradicional escrito en un lenguaje natural, como el español, pero que luego se traduce al código de contrato inteligente. Su objetivo es asegurarles a las partes que en caso de que haya un conflicto, estas puedan acceder a la justicia y hacer cumplir el acuerdo mediante los poderes coercitivos del Estado, a través de sus tribunales. Lo que les permite rescindir o modificar el contrato en ciertos escenarios¹⁹⁹, pero al mismo tiempo también se benefician de la automatización de las cláusulas.

Actualmente, este modelo de contrato inteligente está siendo desarrollado e implementado por varias empresas del sector Blockchain, como es el caso de los contratos inteligentes de Corda del consorcio R3 (que tienen un texto legal de respaldo)²⁰⁰ o la *integración Dual* propuesta por MONAX²⁰¹ o por ERIS INDUSTRIES²⁰².

Existen desafíos técnicos y legales a la hora de elegir este tipo de contratación. Para empezar, la traducción del contrato es un proceso costoso. No todas las cláusulas son susceptibles de representación en código, más bien, como acertadamente advierte LOW, son pocas las obligaciones que pueden automatizarse²⁰³ (como las referentes al pago o transferencia de propiedad que podrían programarse para su ejecución automática), pero una cláusula indemnizatoria, o una cláusula que ordene a los contratantes actuar de buena fe, razonablemente o con debida diligencia, es algo que no puede mecanizarse. Así que necesariamente para ser interpretados requieren de la cognición humana.

¹⁹⁹ DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under Contract Law", *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, p. 76.

²⁰⁰ CLAUSE. (2019). "Smart Legal Contracts on Enterprise Blockchains: A Corda Example". Disponible en: <https://medium.com/inside-r3/smart-legal-contracts-on-enterprise-blockchains-an-r3-corda-example-446957b1b4ba> (fecha de consulta: 4 de octubre de 2020).

²⁰¹ Véase "Legal engineering is the practice of writing smart contracts that automate legally-enforceable rights and obligations". (Sin fecha). Disponible en: https://github.com/monax/legacy-content/blob/master/learn/legal_engineering.md (fecha de consulta: 16 de mayo de 2020).

²⁰² "Putting the Contracts in Smart Contracts". (Sin fecha). Disponible en: <https://erisindustries.com/components/erislegal.html?redirect=true> (fecha de consulta: 3 de octubre de 2020).

²⁰³ LOW, K. & MIK, E. (2019). "Pause the Blockchain Legal Revolution", *International & Comparative Law Quarterly*, Vol. 69, No. 1, p. 170. Disponible en: <https://doi.org/10.1017/S0020589319000502> (fecha de consulta: 3 de enero de 2020).

Asimismo, hay incertidumbre acerca de qué ocurre en caso de una divergencia entre lo expresado en el código y lo acordado por las partes en lenguaje natural, o cómo los contratantes pueden estar seguros de que el lenguaje informático expresa exactamente lo plasmado en el papel, máxime cuando la mayoría de las personas no saben leer ni interpretar el código informático. ¿Será necesaria una nueva figura que sea un híbrido entre un abogado y un programador que certifique la correspondencia entre ambas versiones?

De cualquier modo, estas preocupaciones no son ilegítimas. Una investigación llevada a cabo por investigadores de la Escuela de leyes de la Universidad de Pennsylvania, demostró que en las cincuenta Ofertas Iniciales de Criptomonedas²⁰⁴ (ICO, por sus siglas en inglés *Initial Coin Offering*) de mayor recaudación de 2017, el código *software* que controlaba las ICOs no coincidía, ni reflejaba los términos y condiciones establecidos en lenguaje natural, de tal forma que las promesas de protección a los inversores no se codificaban²⁰⁵.

Por otro lado, ¿Cuál de las versiones tendrá validez en caso de una disputa? Aunque es de suponer que el contrato escrito en lenguaje natural prevalecerá sobre el código, ¿Qué pasa si las partes escogen de común acuerdo que el código prevalecerá sobre el contrato escrito? ¿Cómo lo interpretaría el juez si este no es un experto en lenguaje de *software*? ¿Habrá que hacer una traducción jurada?

La ausencia de estandarización, las múltiples plataformas de contratos inteligentes y la variedad de lenguajes de programación que podemos encontrar para escribir Smart Contracts²⁰⁶, y que incluso se utilizan en una misma plataforma, hace aún más difícil la labor interpretativa por parte de los jueces y de su adopción masiva. Es más, estos lenguajes de programación, a pesar de que fueron creados para escribir contratos

²⁰⁴ Una Oferta Inicial de Criptomonedas, es como un análogo de las ofertas pública de venta (OPV) en el mundo cripto. Generalmente las realiza un proyecto que necesita financiación para desarrollar un producto o servicio Blockchain.

²⁰⁵ COHNEY, S., HOFFMAN, D., SKLAROFF, J. & WISHNICK, D. (2019). "Coin-Operated Capitalism", *Columbia Law Review*, Vol. 119, No. 3, p. 670. Disponible en: https://scholarship.law.upenn.edu/faculty_scholarship/2027 (fecha de consulta: 27 de marzo de 2020).

²⁰⁶ En Ethereum, por ejemplo, hay varios lenguajes de programación como SOLIDITY, VYPER, etc.

inteligentes, no han sido diseñados para capturar el discurso legal, lo que complica aún más su traducción.

Algunos autores han sugerido que una forma de solucionar estos problemas es con la creación de un nuevo lenguaje común de programación que esté diseñado para abordar las características del lenguaje jurídico²⁰⁷, pero como acertadamente señala MIK, el problema es que “la traducción del lenguaje natural en código no constituye un proceso sencillo de convertir el texto legal en instrucciones legibles por computadora, sino que requiere una interpretación previa de ese texto²⁰⁸”, es decir, que se requiere una comprensión de las normas legales, lo cual resulta complejo para un programador. Así que se requiere un enfoque interdisciplinario que incluya a abogados, informáticos y especialistas en áreas comerciales, lo que necesariamente se traduciría costos prohibitivamente altos.

3.3 Hibrido: contrato legal tradicional y código

Este tipo de contrato es un acuerdo escrito en lenguaje natural y código informático, pero solo están escritas en lenguaje de programación las cláusulas que son susceptibles de ejecutarse automáticamente, como, por ejemplo, las cláusulas de pago.

En este modelo el código sería una herramienta que proporcionaría la ejecución automática de algunos apartados del convenio, por lo tanto, no todo el acuerdo sería inteligente, sino solo algunos componentes. En este sentido, el Smart Contract en lugar

²⁰⁷ Véase ISDA & LINKLATERS. (2017). “Whitepaper Smart Contracts and Distributed Ledger – A Legal Perspective”, p. 18. Disponible en: <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> (fecha de consulta: 12 de marzo de 2020), MIK, E. (2017). “Smart contracts: Terminology...”, *cit.*, p. 17, Véase FARMER, W. & HU, Q. (2018). “FCL: A Formal Language for Writing Contracts”, *Quality Software Through Reuse and Integration*, (Drs. RUBIN, S. & BOUABANA-TEBIBEL, T.), Ed.: Springer International Publishing, pp. 190-208. En este sentido, CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). “Smart Contract Templates: essential requirements and design options”, pp. 1 y ss. Disponible en: <https://arxiv.org/abs/1612.04496> (fecha de consulta: 10 de mayo de 2020) proponen la creación de un lenguaje formal que funcione tanto a nivel humano como a nivel de máquina.

²⁰⁸ MIK, E. (2017). “Smart contracts: Terminology, technical limitations and real world complexity”, *Law, Innovation and Technology*, vol 9, No. 2. p. 17. Disponible en: https://ink.library.smu.edu.sg/sol_research/2341 (fecha de consulta: 30 de mayo de 2020).

de ser un contrato per se, sería más bien mecanismo de ejecución²⁰⁹, por lo que serían los términos contractuales subyacentes los que tendrían un efecto legal²¹⁰.

El contrato híbrido puede ser de gran utilidad porque las cláusulas cuya representación en el código generan conflicto como, por ejemplo, ley aplicable, buena fe, debida diligencia, estarían definidas en lenguaje común, y además de que se ofrecerían ganancias de eficiencia. De hecho, esto no es una novedad porque ya se están automatizando los acuerdos marginales que se hacen a partir de la comercialización de contratos de derivados financieros, como pueden ser los colaterales²¹¹, ello se debe a que los pagos y entregas dependen de la lógica condicional, por lo que son fácilmente transponerlos en el código²¹².

Por supuesto, si el código es solo un mecanismo de ejecución, este no excluiría los términos vagos en los acuerdos y habría un componente humano, por lo que muchos defensores de la tecnología argumentarían que se estarían perdiendo las características originales de los Smart Contracts. Sin embargo, las partes pueden sentirse seguras de que el acuerdo refleja fielmente sus intenciones y que es un contrato válido para el derecho.

Consideramos que, por ahora, los acuerdos más básicos o demasiado simples podrían tener completamente automatizadas sus cláusulas, pero como casi todos los contratos requieren un tipo de flexibilidad que se adapte a la realidad cambiante y compleja, estas cláusulas no son adecuadas para su representación y automatización en el código. Es muy posible que la mayoría de los contratos automaticen solo los elementos

²⁰⁹ TAKAHASHI, K. (2018). “Blockchain and Smart Contract...”, *cit.*, p. 5. Véase también LIM, C., SAW, T. & SARGEANT, C. (2016). “Smart Contracts: Bridging the Gap Between Expectation and Reality”. Disponible en: <https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality> fecha de consulta: 17 de abril de 2020).

²¹⁰ CHAMBER OF DIGITAL COMMERCE. (2018). “Smart Contracts” Legal Primer Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable”, p. 2. Disponible en: <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> (fecha de consulta: 29 de febrero de 2019).

²¹¹ ISDA & LINKLATERS. (2017). “Whitepaper Smart Contracts ...”, *cit.*, p. 14. Véase CLACK, C. & MCGONAGLE, C. (2019). “Smart Derivatives Contracts: the ISDA Master Agreement and the automation of payments and deliveries”. Disponible en: <https://arxiv.org/abs/1904.01461> (fecha de consulta: 10 de mayo de 2020).

²¹² DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 77. Al respecto PONCIBÒ, C. & DIMATTEO, L. (2019). “Smart Contracts Contractual and Noncontractual Remedies” *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, p. 120, señala que: “No es de extrañar que los contratos inteligentes hayan dejado su huella por primera vez en las transacciones financieras, ya que las leyes bancarias y financieras se basan en reglas altamente formalizadas”.

que sean capaz hacerlo, lo que implica que los Smart Contracts necesitarán de un contrato “tonto”²¹³ para poder superar las limitaciones técnicas y legales que suponen la representación de un acuerdo en un *software* informático.

3.4 Ricardian contract

Este tipo de contrato fue introducido en la década de los noventa²¹⁴ por el criptógrafo financiero IAN GRIGG, “en un esfuerzo por responder a la pregunta de cómo digitalizar un contrato”²¹⁵. Se trata de un contrato que puede ser fácilmente leído por humanos (como un contrato de papel) porque está escrito en lenguaje natural y también puede ser “leído” por máquinas. Su propósito es ser legalmente vinculante²¹⁶.

El contrato Ricardiano se puede implementar sobre una cadena de bloques²¹⁷ como, por ejemplo, Ethereum, aunque esto no es necesario, ya que puede desarrollarse fuera de Blockchain. Su funcionamiento, explicado de una manera muy básica, se trata de un archivo de texto que se puede leer por humanos y que incluye términos que pueden ser analizados por un *software*. En palabras del propio GRIGG: “es ante todo un documento legible por humanos, y solo en segundo lugar es un documento legible por máquina”²¹⁸. Los contratantes firman criptográficamente el acuerdo, luego este se registra en la cadena de bloques y se le asigna un *hash* (un número único)²¹⁹.

Es un contrato semiautomático, los términos que no se puedan representar en la lógica formal del código quedan escritos en lenguaje natural, por lo que deben ser

²¹³STARK, J. (2016). “Making Sense of Blockchain Smart Contracts”. Disponible en: <https://www.coindesk.com/making-sense-smart-contracts> (fecha de consulta 2 de febrero de 2020). Ver DUROVIC, M. & JANSSEN, A. (2019). “Formation of Smart Contracts under ...”, *cit.*, p. 77.

²¹⁴GRIG, I. (1998-2000). “Financial Cryptography in 7 Layers”. Disponible en: <https://iang.org/papers/fc7.html> (fecha de consulta: 20 de agosto de 2019).

²¹⁵R3. (2017). “What is a Ricardian contract”. Disponible en: <https://www.r3.com/blog/what-is-a-ricardian-contract/> (fecha de consulta: 28 de agosto de 2020).

²¹⁶GRIG, I. (Sin fecha). “The Ricardian Contract”. Disponible en: <https://iang.org/ricardian/> (fecha de consulta: 20 de agosto de 2019).

²¹⁷“How Are Ricardian Contracts Different From Smart Contracts?”. (2021). Disponible en: <https://learn.bybit.com/defi/how-are-ricardian-contracts-different-from-smart-contracts/> (fecha de consulta: 3 de enero de 2022).

²¹⁸GRIGG, I. (2017). “Towards A Ricardian Constitution”. Disponible en: <https://steemit.com/eos/@iang/towards-a-ricardian-constitution> (fecha de consulta: 26 de agosto de 2019).

²¹⁹“Ricardian contracts: A smarter way to do smart contracts?”. (Sin fecha). Disponible en: <https://www.schoenherr.eu/publications/publication-detail/ricardian-contracts-a-smarter-way-to-do-smart-contracts/> (fecha de consulta: 17 de agosto de 2020).

ejecutados por los humanos, por ello se habla de que su ejecución es semiautomática, porque solo algunas cláusulas pueden ser autoejecutadas.

Actualmente, en varios sectores se está experimentando con la utilización de este tipo de contratos como, por ejemplo, Open Bazar²²⁰, una plataforma Blockchain de comercio electrónico, CommonAcord²²¹, ISDA (por sus siglas en inglés, International Swaps And Derivatives Association)²²², entre otros.

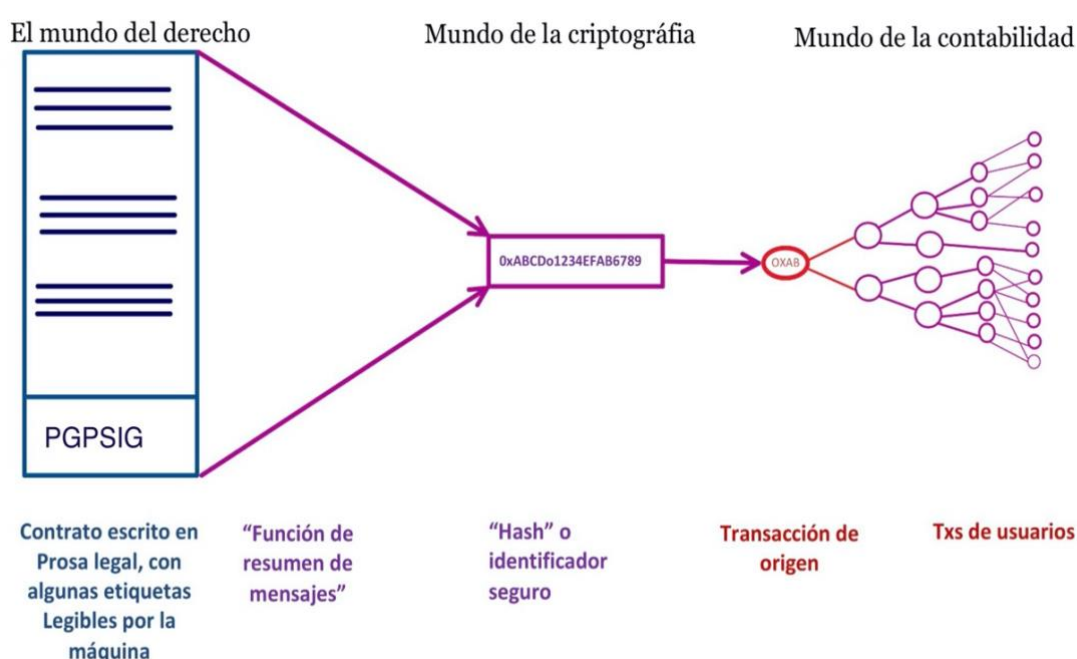


Figura No. 2. El documento jurídico se firma digitalmente, y sobre ese contenido se genera un *hash* o identificador único y seguro, luego este se registra en la Blockchain. Adaptado de DE OLIVEIRA, F., GRIGG, I., PEREIRA, R. & CARCAZERE, L. (2017). “Triple entry ledgers with blockchain for auditing” *International Journal of Auditing Technology*, Vol. 3, no 3, p. 169. Disponible en: <https://doi.org/10.1504/IJAUD. IT.2017.086741> (fecha de consulta: 12 de septiembre de 2020).

²²⁰“Ricardian Contracts in OpenBazaar”. (Sin fecha). Disponible en: <https://gist.github.com/drwash0/a5380544c170bdbbbad8> (fecha de consulta: 17 de agosto de 2020). Esta plataforma cerró a inicios de 2021.

²²¹ HAZARD, J. & HAAPIO, H. (2017). “Wise Contracts: Smart Contracts that Work for People and Machines”. *Trends and communities of legal informatics. Actas del 20th international legal informatics symposium IRIS*. Disponible en: <https://ssrn.com/abstract=2925871> (fecha de consulta: 20 de abril de 2020).

²²² ISDA. (2018). “ISDA Publishes Digital Iteration of the Common Domain Model”. Disponible en: <https://www.isda.org/2018/06/05/isda-publishes-digital-iteration-of-the-common-domain-model/> (fecha de consulta: 17 de agosto de 2020).

4. Contratos legales inteligentes

Luego de analizar los tipos de contratos inteligentes, volvemos hacer la pregunta de si los Smart Contracts pueden superar las limitaciones legales y técnicas para ser legalmente exigible. La respuesta es que algunos tipos de contratos si, y otros no. Bajo ciertas condiciones y, si las partes deciden estar vinculadas contractualmente, pueden celebrar acuerdos que cumplan con los requisitos legales. En efecto, la legislación española estipula que se puede prestar un consentimiento válido por dispositivos automáticos²²³, lógicamente, ello implicaría una renuncia a la “filosofía libertaria” de esta tecnología.

Asimismo, de acuerdo a lo observado en párrafos anteriores, hoy en día no se cuenta con los medios técnicos para codificar totalmente un contrato legal con todos sus conceptos jurídicos complejos, por tal razón, los Smart Contracts de algunas plataformas que pretenden que sus contratos tengan efectos legales, incorporan un contrato subyacente escrito en lenguaje natural, o también se utilizan como herramientas para codificar partes del acuerdo.

Quizás en un futuro los contratos inteligentes sigan un camino similar a al Intercambio Electrónico de Datos, debido a las limitaciones de representación de cláusulas ambiguas Como acertadamente señalan DE FILIPPI y WRIGHT “Con EDI, las partes optan por no depender de arreglos completamente basados en códigos, sino que ejecutan acuerdos maestros que contextualizan el uso de mensajes electrónicos en el contexto de una relación contractual más amplia.”²²⁴. La combinación de lenguaje natural y código, dota al contrato de los beneficios de la utilización de cada tipo: la flexibilidad del lenguaje natural, y la ejecución automática y a prueba de manipulaciones del código.

No obstante, los jueces y los legisladores, más pronto los primeros que los segundos, se verán en la necesidad de dar respuestas a estos asuntos, porque si bien, hoy en día, gracias a su empleo experimental, no se trasladan muchas disputas a los tribunales,

²²³ España. Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, *Boletín Oficial del Estado*, 11 de julio de 2002.

²²⁴ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 78.

cuando su uso se extienda, es muy probable que se presenten una cantidad ingente de demandas de contratos inteligentes.

4.1 ¿Cómo deberían ser los contratos inteligentes?

Los contratos inteligentes, al menos por ahora, están siendo usados en gran parte de forma experimental y marginal, debido a que son lentos y costosos. Generalmente, se desenvuelven en entornos informales y de emprendedores, ello implica que tengan problemas de control de calidad²²⁵, errores en su código o que sean víctima de ataques de piratería.

Si bien, en algunos puntos específicos mejoran la eficiencia y reducen las posibilidades de incumplimiento, no logran eliminar del todo los conflictos, porque el código también es susceptible de error²²⁶. En ausencia de una regulación específica que delimite responsabilidades de estos fallos y en escenarios de contratación anónima, los usuarios de estos contratos deben ser conscientes de los riesgos que suponen celebrar acuerdos sin recursos ni remedios para afrontar esos errores²²⁷.

A continuación, expondremos una propuesta de cómo podrían aplicarse los Smart Contracts en un contexto seguro para que sean legalmente vinculantes, desde luego, es una proposición desde un enfoque hipotético, porque con el avance de la tecnología y sin una estandarización de la industria, en realidad no sabemos cómo se verán en un futuro las implementaciones exitosas de contratos inteligentes²²⁸, si es que lo hacen. No es una fórmula mágica, pero consideramos que para mitigar el riesgo deberían contar con estas tres características:

²²⁵ COHNEY, S., HOFFMAN, D., SKLAROFF, J. & WISHNICK, D. (2019). "Coin-Operated ...", *cit.* p. 659.

²²⁶ Incluso pueden ser por incumplimiento que sea por hechos que tengan lugar fuera de la cadena de bloques, como, por ejemplo, si se tiene que entregar un producto en físico y no este no se efectúa.

²²⁷ CIEPLAK, J. & LEEFATT, S. (2017). "Smart Contracts: A Smart Way ...", *cit.*, p. 425.

²²⁸ CLIFFORD CHANCE. (2017). "Are smart contracts contracts?", p. 2. Disponible en: <https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/are-smart-contracts-contracts.html> (fecha de consulta: 9 de abril de 2020).

i. La vinculación de un contrato escrito en lenguaje natural

Como observamos anteriormente, envolver el código en un contrato de papel es una forma de estar seguros de la exigibilidad legal del código en caso de una disputa. También se pueden incorporar en el texto escrito en lenguaje natural las cláusulas que no son adecuadas para su representación en el código por ser de carácter ambiguo o contener conceptos indeterminados.

ii. Prioridad del contrato escrito sobre el código

Se debe dejar por escrito que el contrato tradicional tendrá prioridad sobre lo estipulado en el código, pues en caso de que existan discrepancias se evitan problemas con el significado del mismo. Esto se debe, en parte, porque es bastante probable que las partes no comprendan el lenguaje de programación.

iii. Posibilidad de modificación

A pesar de que esta posibilidad puede aniquilar con una de las principales ventajas que ofrece la tecnología, como es lo es la inmutabilidad, consideramos que los contratos inteligentes deben ser susceptibles de modificación o rectificación²²⁹, ya sea por un error de codificación del código (que puede ser bastante común), por común acuerdo de las partes, por hechos sobrevinientes, o porque quizás sea necesaria la intervención de un tribunal para dirimir una controversia.

Desde luego, la facultad de modificar o rescindir el contrato debe estar codificada de antemano en el código, dada la imposibilidad de parcheo²³⁰ de los Smart Contracts²³¹. Otra posibilidad de modificación, es que las partes realicen una nueva transacción que

²²⁹ Dicha posibilidad de modificación debe codificarse o permitirse en el código desde el principio, véase WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *cit.*, p.123.

²³⁰ En informática, un parche son los cambios que se le aplican a un *software* para mejorarlo, solucionar problemas, introducir funcionalidades, entre otros.

²³¹ JIAO J., LIN SW., SUN J. (2020) "A Generalized Formal Semantic Framework for Smart Contracts", Lecture Notes in Computer Science, vol 12076, p. 75. Disponible en: https://doi.org/10.1007/978-3-030-45234-6_4 (fecha de consulta: 15 de diciembre de 2020). Advierte SAYEED, S., MARCO-GISBERT, H. y CAIRA, T. (2020). "Smart Contract: Attacks and Protections". *Ieee Access*, Vol. 8, Disponible en: <https://ieeexplore.ieee.org/document/8976179> (fecha de consulta: 15 de diciembre de 2020), que "los contratos inteligentes se desarrollan de una manera distinta al *software* tradicional. Una vez implementado en Blockchain, un contrato inteligente no se puede modificar ni actualizar para parches de seguridad".

interactúe con el contrato original, para revertir los resultados no deseados del contrato defectuoso²³².

La multiplicidad de obstáculos legales y técnicos que suponen la implementación pura de un contrato inteligente requieren que para garantizar su seguridad jurídica se efectúen cambios de diseño, lo cual implica un abandono de sus características más fascinantes, como lo son la inmutabilidad o la ejecución automática. Desde luego, ello comporta un menor atractivo para la adopción de esta tecnología, lo que nos hace pensar si las famosas ganancias de eficiencia superan los costos que debemos asumir.

5. Algunos desafíos jurídicos: errores de codificación

Como hemos mencionado, existen una serie de desafíos jurídicos que los contratos inteligentes deberán abordar, pero consideramos, que uno de los más fundamentales y con mayor relevancia, es la presencia de errores de codificación o *bugs*, cuyas consecuencias pueden ser incluso catastróficas, como el caso del DAO, donde alguien vilmente explotó un error de programación, logrando defraudar más de 50 millones de dólares, pero, ¿qué sucede jurídicamente, si el algoritmo está mal programado y los resultados no son los esperados por los contratantes?, ¿Podemos hablar de incumplimiento en caso de que el código contenga algún error y las obligaciones no se ejecuten, o se ejecuten de forma incorrecta y ello genere perjuicios para una o ambas partes?, pero, si hablamos de incumplimiento, ¿por parte de quién?, ¿Quién es el responsable?, ¿el programador? ¿cómo podemos responsabilizar al código?

Se ha dicho que la ejecución de las obligaciones está garantizada porque el código se ejecuta según lo programado, al respecto, autores como LEGERÉN MOLINA afirman que los contratos inteligentes “eliminan el incumplimiento: no es que faciliten el cumplimiento de lo establecido, lo hacen inevitable”²³³. No obstante, creemos que esta es una afirmación casi utópica, en el entendido que la redacción del contrato debería ser perfecta y no contener ningún error. No debemos olvidar, que al final de cuenta un Smart

²³² PONCIBÒ, C. & DIMATTEO, L. (2019). “Smart Contracts Contractual ...”, *cit.*, p. 130.

²³³ LEGERÉN-MOLINA, A. (2020). “Smart Contracts que...”, *cit.*, p. 291.

Contract es un programa informático que está redactado por humanos y como tal, puede presentar errores.

Si bien, el contrato tiene asegurada su ejecución a través de los nodos de la red Blockchain, como acertadamente señala MIK, las cadenas de bloques no pueden garantizar que el código represente correctamente la obligación subyacente²³⁴, pues el mecanismo de consenso solo verifica de si las transacciones siguieron o no las reglas del código.

5.1 Errores de codificación en Ethereum

Ethereum es una de las plataformas más famosa para la creación y ejecución de contratos inteligentes, sin embargo, varios estudios²³⁵ han demostrado que sus contratos contienen fallos de diseños y son susceptibles a ataques piratas²³⁶; lo que conllevan al cumplimiento defectuoso de las obligaciones.

Las vulnerabilidades algorítmicas de los Smart Contracts apenas están siendo conocidas por los tecnólogos, pero los atacantes están aprovechando dichos agujeros de seguridad para desplegar su actividad criminal, ello ha ocasionado pérdidas de dinero a las empresas, incluso, si no hay ataques intencionados. Como prueba de ello, un grupo de investigadores²³⁷ que analizó cerca de un millón de contratos inteligentes desplegados en

²³⁴ MIK, E. (2019). "Smart Contracts: A Requiem", *Journal of Contract Law*, p. 8. Disponible en: <https://ssrn.com/abstract=3499998> (fecha de consulta: 4 de mayo de 2020).

²³⁵ Véase NIKOLIĆ, I., KOLLURI, A., SERGEY, LL., SAXENA, P. & HOBOR, A. (2018). "Finding the greedy, prodigal, and suicidal contracts at scale", *Proceedings of the 34th Annual Computer Security Applications Conference*, P. 653. Disponible en: <https://doi.org/10.1145/3274694.3274743> (fecha de consulta: 12 de noviembre de 2020), ATZEI, N., BARTOLETTI, M., & CIMOLI, T. (2017). "A survey of attacks on ethereum smart contracts sok", *International conference on principles of security and trust*, pp. 164-186, Springer, Berlin. Disponible en: https://dl.acm.org/doi/10.1007/978-3-662-54455-6_8 (fecha de consulta: 10 de mayo de 2020). Ver CHEN, H., PENDLETON, M., NJILLA, L., & XU, S. (2020). "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses", *ACM Computing Surveys*, Vol. 53, No. 3. Disponible en: <https://dl.acm.org/doi/fullHtml/10.1145/3391195> (fecha de consulta: 15 de noviembre de 2020).

²³⁶ En este sentido señala QURESHI, H. (2017). "A hacker stole \$31M of Ether — how it happened, and what it means for Ethereum". Disponible en: <https://www.freecodecamp.org/news/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce/> (fecha de consulta 12 de octubre de 2020), que, "el código de los contratos inteligentes de Ethereum es público por defecto, ello implica que cualquier pirata pueda darse cuenta del error y explotarlo. Aunque el programador puede especificar que su visibilidad sea privada, muchas veces se le olvida hacerlo privado. Un buen ejemplo de ello fue el ataque que sufrió la billetera Parity en la cual un hacker logró extraer de forma ilegal 31 millones de dólares, que hubiesen podido ser más, pero gracias a la actuación del grupo de desarrolladores, The White Hat Group, se logró detener el ataque. Según expertos, el w era una vulnerabilidad del contrato inteligente, un error de programación que le permitió a los atacantes reiniciar la billetera y establecerse como los nuevos propietarios, para luego marcharse con todo el dinero".

²³⁷ NIKOLIĆ, I., KOLLURI, A., SERGEY, LL., SAXENA, P. & HOBOR, A. (2018). "Finding the greedy, prodigal...", *cit.*, p. 653.

Ethereum, encontró que 34.200 contratos (de los cuales, 2365 eran distintos) contenían errores.

Según CRYPTONICS²³⁸, una empresa de ciberseguridad que audita contratos inteligentes relacionados con pólizas de seguros, fondos de inversión, plataformas descentralizadas, entre otros; se identificaron cinco fallas comunes tales como, errores aritméticos relacionados con números enteros, reversión por falta de gas, ausencia de comprobaciones esenciales que ocasionan que la operación no sea válida, por ejemplo, no verificar que un usuario tenga suficiente saldo de tokens para ejecutar una determinada operación, el adelanto de una transacción no confirmada y errores de lógica simple, que según CRYPTONICS, es el error más común de los contratos inteligentes. El famoso ataque de la DAO es un buen ejemplo de este tipo de error.

Las cadenas de bloques tienen características y vulnerabilidades únicas²³⁹, que conllevan a consecuencias desastrosas, como apropiadamente expresa ORCUTT, el *hack* del DAO, es el mejor ejemplo para ilustrarlo, en el *software* tradicional, un error se puede solucionar con un parche. En el mundo Blockchain, no es tan simple, porque las transacciones en una cadena de bloques no se pueden revertir porque son inmutable. Continúa explicando el autor que, aunque los errores no pueden ser corregidos directamente en el código del contrato mediante un parche, pueden ser mejorados con la creación de otros Smart Contracts que interactúen con ellos. Es decir, hay que reemplazar el contrato por uno nuevo y vincularlo con el antiguo. Por supuesto, de nuevo hay que pagar las tarifas de transacción para poder implementarlo. Otra solución es un *kill switches*²⁴⁰ (interruptor de apagado, en español) centralizado en una red para detener toda

²³⁸BEYER, S. (2020). "The 5 Most Common Smart Contract Vulnerabilities". Disponible en: <https://medium.com/cryptonics/the-5-most-common-smart-contract-vulnerabilities-738de4fae3ba> (fecha de consulta: 12 de noviembre de 2020). Según ORCUTT, desde principios de 2017 (hasta principio de 2019, fecha de publicación del artículo) "los piratas informáticos han robado cerca de \$ 2 mil millones de dólares en criptomonedas, esto son solo atacantes que actúan en solitario u oportunista, pero las organizaciones cibercriminales también están aprovechando las vulnerabilidades y se calcula que probablemente han robado mil millones de dólares".

²³⁹ ORCUTT, M. (2019). "Once hailed as unhackable, blockchains are now getting hacked", *MIT Technology Review*, Disponible en: <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> (fecha de consulta: 19 de noviembre de 2020).

²⁴⁰ Un *kill switch* o interruptor de apagado, en español, es una medida de seguridad para interrumpir o apagar de emergencia la ejecución de un programa, se usa habitualmente para detener un robo de dinero o datos.

la actividad, una vez se detecta el ataque. No obstante, será demasiado tarde para recuperar el dinero que ha sido robado.

Explica ORCUTT, que solo hay una forma de recuperar el dinero, y es reescribir la Blockchain para volver al punto previo al ataque, mediante un *Hard Fork* (bifurcación dura) para crear una nueva cadena, previa aprobación de la mayoría de los nodos, recordemos que justamente esto fue lo que hizo Ethereum para solucionar los problemas del DAO.

Evidentemente, es prácticamente improbable que esto vuelva a ocurrir o que suceda en contratos más pequeños. Esto solo sería posible en un escenario en el que “el código subyacente esté lo suficientemente extendido como para afectar negativamente a un gran número de participantes”²⁴¹, es decir, que muchos miembros hayan sufrido pérdidas por la ejecución defectuosa de un Smart Contract, ya que requiere que la mayoría de los nodos de la red Blockchain cooperen para realizarlo.

5.2 Sentencia B2C2 vs Quoine

Febrero de 2020, el Tribunal de apelaciones de Singapur tuvo que dirimir una controversia en relación con los fallos que puede presentar el código cuando se ejecutan contratos de forma automática. Es importante subrayar que la decisión se tomó basándose en el al derecho consuetudinario o *commonlaw*, pero, creemos que al ser una de las primeras decisiones que involucra criptomonedas y contratos inteligentes, servirá como una guía sobre las futuras controversias de este tipo que se puedan presentar en cualquier clase de sistema jurídico.

5.2.1 *Elementos facticos*

Demandante: B2C2 LTD Demandado: Quoine Pte LTD. Quoine operaba a través de una plataforma de intercambio de criptomonedas (*Exchange*), llamada

²⁴¹ Véase VERSTRAETE, M. (2019). “The Stakes of Smart Contracts”, *cit.*, p. 777, de igual forma KOLBER, A. (2018). “Not-so-smart blockchain contracts and artificial responsibility”, *Stanford Technology Law Review*, Vol. 21, p. 226. Disponible en: <https://law.stanford.edu/publications/not-so-smart-blockchain-contracts-and-artificial-responsibility/> (fecha de consulta: 21 de mayo de 2020) señala que, “las bifurcaciones duras probablemente serán más difíciles de lograr en el futuro. A medida que la red Ethereum crece y cualquier contrato inteligente o DAO en particular representa un porcentaje cada vez menor del ecosistema, las partes interesadas de Ethereum pueden volverse cada vez más reacias a bifurcar para corregir errores”.

QUOINEExchange y B2C2 cotizaba en dicha plataforma²⁴². Las partes, Quoine y B2C2 eran creadoras de mercado, es decir, garantizaban la liquidez de la plataforma comprando y vendiendo criptomonedas, con lo que ayudaban a minimizar las fluctuaciones de los precios de las criptomonedas en dicha plataforma. El demandante había celebrado un contrato con la demandada en virtud del cual B2C2 podía realizar intercambios de criptomonedas con otras contrapartes en la plataforma de Quoine²⁴³.

Los contratos de compra y venta se celebraban de forma automática sin ninguna intervención humana, a través de los algoritmos deterministas creados por ambas partes²⁴⁴. Por un lado, *Program Quoter*, propiedad de Quoine, era responsable de operar la plataforma y recuperar (actualizar) los precios de mercado²⁴⁵, y, por otro lado, *Pure Quote*, un programa de negociación algorítmica, propiedad de B2C2, diseñado por el director de dicha compañía, para ser operado con una mínima intervención humana. Además, es importante destacar que dicho *software* era de carácter determinista, es decir, la misma entrada siempre produciría exactamente la misma salida. En otras palabras, el programa de computador de negociación se ejecutaría según lo estipulado en el código de programación y no tenía la capacidad de desarrollar sus propias respuestas frente a condiciones variables²⁴⁶.

Sin embargo, algo salió mal. El 19 de abril de 2017 debido a una negligencia, Quoine no implementó ciertas actualizaciones necesarias en su *software* de cotización, *Program Quoter*, por lo que el programa no estaba funcionando correctamente. Como consecuencia, B2C2 vendió el Ether (*ETH*) a cambio de Bitcoin (*BTC*), a otros usuarios de la plataforma, Pulsar Trading Capital y al Sr. Yu Tomita, a una tasa de 9.99999 *BTC* o 10 *BTC* por 1 *ETH*²⁴⁷. Lo que significaba que el *Ether* se vendió aproximadamente 250

²⁴² CORTE DE APELACIONES DE LA REPUBLICA DE SINGAPUR. (2019) Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia de 24 de febrero de 2020. Disponible en: <https://tinyurl.com/y5r6w9sd> (fecha de consulta: 1 de diciembre de 2020).

²⁴³ NORTON ROSE FULBRIGHT. (2019). "Singapore court's cryptocurrency decision: Implications for cryptocurrency trading, smart contracts and AI". Disponible en: <https://www.nortonrosefulbright.com/en-nl/knowledge/publications/6a118f69/singapore-courts-cryptocurrency-decision-implications-for-trading-smart-contracts-and-ai> (fecha de consulta: 1 de diciembre de 2020).

²⁴⁴ Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia.

²⁴⁵ LOW, K. & MIK, E. (2020). "Lost in Transmission: Unilateral Mistakes in Automated Contracts", *Law Quarterly Review*. Disponible en: <https://ssrn.com/abstract=3591657> (fecha de consulta: 1 de diciembre de 2020).

²⁴⁶ Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia.

²⁴⁷ Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia.

veces la tasa vigente del mercado de ese momento, dejando a BTC2 con una ganancia inesperada²⁴⁸.

Al día siguiente de realizado el intercambio, cuando Quoine se enteró, consideró que las tasas eran muy anormales y procedió unilateralmente cancelar y revertir las operaciones, a pesar de que el contrato estipulaba que las operaciones eran irreversibles.

5.2.2 *La controversia*

Mientras B2C2 inició un proceso contra Quoine en el entendido que las operaciones revertidas constituían un incumplimiento del contrato y un abuso de confianza por parte de Quoin. Por su parte, Quione argumentó que no había incumplimiento de contrato, que en caso de que lo hubiese, los contratos comerciales eran nulos por error unilateral²⁴⁹ y que B2C2 se enriquecería injustamente a expensa de otros.

5.2.3 *Problema jurídico*

El tribunal debía determinar el tipo conocimiento de la parte que no cometió el error (en este caso, B2C2), cuando las transacciones se ejecutan según lo programado en su código (determinista) y sin ningún tipo de intervención humana, debido a que, en *el commonlaw*, para que opere la doctrina del error unilateral, la parte no equivocada debe tener conocimiento de dicho error para que el contrato pueda declararse nulo.

5.2.4 *Decisión*

El Tribunal falló a favor de B2C2 y declaró responsable a Quoine por incumplimiento contractual y abuso de confianza por revertir y cancelar unilateralmente las operaciones objeto del litigio.

La Audiencia no aplicó la doctrina del error unilateral, en el entendido que consideró que era fundamental examinar el estado de conocimiento del desarrollador del

²⁴⁸ FU, J. (2020). “Algorithmic contracts: who is to blame?”, *Singapore Law Review*, Vol. 12. Disponible en: <https://www.singaporelawreview.com/juris-illuminae-entries/2020/algorithmic-contracts> ((fecha de consulta: 1 de diciembre de 2020).

²⁴⁹ En derecho inglés un error unilateral consiste cuando una de las partes comete un error, mientras que la otra parte es consiente de ese error.

algoritmo al momento de la programación, y no en el momento posterior a la redacción. De tal forma que, si había una falla, el *software* Pure Quote no lo sabía, porque este solo ejecutaba las órdenes preprogramadas en su código. El error unilateral solo se hubiese aplicado si B2C2 hubiera previsto un posible error de codificación por parte de Quoine y hubiera diseñado su programa (Pure Quote), para explotar dicho fallo. No obstante, el Tribunal consideró que el programador de B2C2 no poseía ni debía poseer tal conocimiento.

Asimismo, el Tribunal tampoco admitió que existía un enriquecimiento sin causa por parte de B2C2, debido a que los *BTC* se acreditaron de conformidad a contratos válidos celebrados entre las partes²⁵⁰.

5.3 Conclusiones del caso

Si los contratos inteligentes se hubieran ejecutado en una cadena de bloques hubiera resultado ser más compleja la reversión de las transacciones²⁵¹ y la materialización de la decisión del Tribunal, situación que se hubiera tornado más compleja si las partes hubiesen permanecido seudónimas. Primero, porque para presentar la demanda se debe conocer la identidad de la contraparte. Segundo, porque para modificar los resultados de las transacciones erróneas, es menester de una segunda transacción para realizar tal modificación. Pero la cuestión aquí relevante son las consecuencias jurídicas de la presencia de bugs en la codificación.

Creemos que el incumplimiento de las obligaciones contractuales, cuando sea por causas imputable al código por un error de programación o incluso pirateos, debería tener un nuevo tratamiento jurídico, pues si aplicamos este concepto de acuerdo a los preceptos tradicionales del derecho contractual se van a generar muchas problemáticas de cara a establecer responsabilidades.

Habida cuenta de que los contratantes no pueden interferir en el desempeño de las obligaciones programadas en el código subyacente, consideramos que, si la inobservancia de lo estipulado en el acuerdo no puede ser atribuible a una de las partes, porque es

²⁵⁰ Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia.

²⁵¹ Esta posibilidad de modificación debía estar codificada en el contrato.

consecuencia directa de un error de codificación, no podemos calificarlo como incumplimiento. En este sentido, hay quienes han advertido, en la doctrina, que debemos hablar de mal funcionamiento²⁵². No obstante, la cuestión aquí es que debemos determinar quién responde frente al incumplimiento y cuál será la suerte que correrá el contrato.

La decisión del Tribunal de Apelaciones de Singapur fue tomada con base en una adaptación de las normas y principios legales a un contexto sumamente novedoso, como lo son, los contratos que se celebran de forma automática y sin la intervención humana. No obstante, es necesaria la existencia de remedios legales que subsanen estos errores bajo los criterios de la justicia material, porque como pudimos observar, ello no ocurrió en dicho fallo. Pensemos, por ejemplo, si la operación hubiera tenido participación de consumidores finales, lógicamente, estos hubieran resultado perjudicados.

La ley debe adaptarse a las nuevas realidades tecnológicas y en este contexto es necesario un marco jurídico apropiado que determine los derechos y obligaciones de las partes, asigne responsabilidades y se adapte a las fallas algorítmicas que pueden presentar los contratos inteligentes²⁵³, máxime por los avances del aprendizaje automático, que hace más notoria esta necesidad, ya que el código es no determinista, es decir, una misma entrada puede producir diferentes salidas, lo que significa que el código se va reescribiendo solo.

6. Responsabilidad por errores de programación

Llegados a este punto, debemos pensar en la asignación de responsabilidades cuando las obligaciones no se ejecutan, o se ejecutan de forma defectuosa debido a los errores de programación, o por la presencia de vulnerabilidades que hacen al contrato blanco de ataques por parte de piratas, teniendo en cuenta, de que pueden conllevar a importantísimas pérdidas económicas.

Son muchas las partes involucradas en el correcto funcionamiento de un contrato inteligente, a saber, (i) los desarrolladores de la plataforma Blockchain, que son los

²⁵² MIK, E. (2017). "Smart contracts: Terminology...", *cit.*, p. 11.

²⁵³ LOW, K. & MIK, E. (2019). "Pause the Blockchain Legal ...", *cit.*, p. 169.

encargados del mantenimiento del ecosistema²⁵⁴; (ii) los programadores de los contratos inteligentes, los mineros o validadores que validan las transacciones²⁵⁵ y; por último, (iii) los usuarios, quienes realizan las transacciones ²⁵⁶.

Los desarrolladores de la plataforma y los mineros, en principio, no deberían responder por la presencia de errores de un contrato, pues ellos no están involucrados directamente en su desarrollo. Sin embargo, si el error no fuese por el contrato, sino por un fallo de la plataforma donde este se encuentra alojado, sería complejo asignar responsabilidades, dado que, el *software* que está detrás de las Blockchains públicas normalmente es de código abierto, lo que significa que es desarrollado de forma colectiva.

En este orden de ideas, la responsabilidad recaerá sobre el desarrollador o los contratantes. No obstante, las partes tampoco deberían responder cuando el error es causado por un tercero²⁵⁷. De tal manera que, solo nos queda responsabilizar al programador, que según COMELLES²⁵⁸, para individualizar su conducta, la responsabilidad debería tener carácter subjetivo conforme a lo establecido en el artículo 1902 del Código Civil²⁵⁹.

La función del desarrollador del contrato inteligente consiste en codificar las obligaciones que los contratantes le han indicado, de tal manera que “están tomando (...) decisiones sobre cómo se aplicarán (estas obligaciones²⁶⁰) en la práctica, lo que puede significar que tienen mayores responsabilidades legales²⁶¹”. Es decir, su labor afectará la

²⁵⁴ Los desarrolladores se encargan de programar el código en una Blockchain.

²⁵⁵ Los mineros o validadores son lo que se encargan de agregar nuevos bloques y validar las transacciones, de acuerdo al protocolo de consenso.

²⁵⁶ Esta clasificación fue propuesta por el comisionado de la Comisión de Negociación de Futuros de Productos Básicos de Estados Unidos, ver QUINTENZ, B. (2018). “Remarks of Commissioner”, *38th Annual GITECH Technology Week Conference*. Disponible en: <https://cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16> (fecha de consulta: 18 de septiembre de 2020).

²⁵⁷ GIANCASPRO, M. (2017). “Is a ‘smart contract’ really ...”, *cit.*, p. 829.

²⁵⁸ COMELLES, C. (2020). “Smart contracts o Code is Law: soluciones legales para la robotización contractual *InDret: Revista para el Análisis del Derecho*, no 4, p. 25. Disponible en: <https://indret.com/smart-contracts-o-code-is-law-soluciones-legales-para-la-robotizacion-contractual/> (fecha de consulta: 20 de noviembre de 2020).

²⁵⁹ Artículo 1902. El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

²⁶⁰ Subrayado fuera del texto.

²⁶¹ BOUCHER, P., NASCIMENTO, S., & KRITIKOS, M. (2017). *Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques*. Brussels: European Parliament. p. 16. Disponible en: http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0217043ESN (fecha de consulta: 19 de septiembre de 2019).

condición legal de las partes durante la vigencia del contrato y, por lo tanto, deben asumir responsabilidades, siempre y cuando el error le sea imputable, porque el contrato también puede ser víctima de un ataque pirata.

7. ¿Qué sucede con el contrato?

Creemos imprescindible que debemos dejar claro que, los contratos inteligentes que tengan por objetivo ser legalmente vinculantes deben estar sometidos a las leyes y sujetos a la ejecución judicial²⁶², porque el código no es la ley. Todo ordenamiento jurídico reconoce que la ejecución del contrato puede fallar por diferentes motivos, sin por ello tener que responsabilizar al deudor por el incumplimiento del contrato²⁶³. Así que, debido a la imposibilidad de las partes de prever todos los eventos futuros, se aplicarán las normas del derecho contractual.

Según la legislación española, cuando el cumplimiento del contrato se vuelve imposible como consecuencia de un hecho sobrevenido, imprevisto e inevitable, el deudor queda exonerado de toda responsabilidad en los términos de los artículos 1105²⁶⁴, 1182²⁶⁵ y 1184²⁶⁶ del código civil. En algunos casos, el deudor queda exonerado de responsabilidad por los daños y perjuicios, y en otros casos, además también del cumplimiento de la obligación, dependiendo si es fuerza mayor o caso fortuito²⁶⁷. Es decir, la exoneración de responsabilidad del deudor se da, porque la causa que imposibilita o frustra el cumplimiento de la prestación no es su culpa.

²⁶² En este sentido, advierten DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 78 que, “los tribunales conservan la jurisdicción sobre los efectos legales de un contrato inteligente. Ellos interpretarán el código subyacente de acuerdo con principios de larga data de interpretación del derecho contractual y, si es necesario, con la ayuda de expertos. ”. Una opinión, acertada, a la que nos sumamos.

²⁶³ TJONG TJIN TAI, E. (2018). "Force majeure and excuses in smart contracts", *Tilburg Private Law*, documento de trabajo, No. 10., p. 5. Disponible en: <http://dx.doi.org/10.2139/ssrn.3183637> (fecha de consulta: 10 de septiembre de 2020).

²⁶⁴ Fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables.

²⁶⁵ Quedará extinguida la obligación que consista en entregar una cosa determinada cuando ésta se perdiere o destruyere sin culpa del deudor y antes de haberse éste constituido en mora.

²⁶⁶ También quedará liberado el deudor en las obligaciones de hacer cuando la prestación resultare legal o físicamente imposible.

²⁶⁷ El Tribunal Supremo en sentencia del 22 de Diciembre de 1997, ha señalado que “esta distinción es de origen doctrinal, “Ante todo hay que poner de manifiesto que no existe en nuestro derecho una definición de la fuerza mayor distinguiéndola del caso fortuito, puesto que en el artículo 1105 del Código Civil se establece una regulación omnicomprendensiva de ambos supuestos, en la que se exige, como señala el precepto, que estemos en presencia de sucesos que no hubieran podido preverse o que previstos fueran inevitables. La distinción es de origen doctrinal y

Asimismo, en la contratación con consumidores, durante la emergencia de la COVID-19, se introdujeron en la legislación española de forma transitoria medidas de protección²⁶⁸ de los consumidores, para paliar los efectos de la pandemia, como el derecho de resolución en algunos contratos sin penalización (compraventa de bienes y prestación de servicios), cuando su cumplimiento resulte imposible. La norma señala que, el usuario tiene la potestad de resolver el contrato en un plazo de 14 días, siempre y cuando, no se pueda obtener de la propuesta de revisión (como bonos o vales sustitutorios al reembolso) una solución que restaure la reciprocidad de intereses del contrato. No obstante, la medida no le otorga al consumidor la posibilidad de resolver el contrato de forma inmediata, sino que está supeditado a que no haya acuerdo entre las partes, sobre la propuesta de revisión en el transcurso de 60 días. Es decir, que el ejercicio de este derecho, queda suspendido y limitado a una serie de condiciones. En este sentido, TORRELLES advierte acertadamente que la disposición obliga “al consumidor a que reconsidere la conveniencia de una prestación alternativa razonable de cumplimiento para conservar el contrato”²⁶⁹, lo que evidentemente es, tal y como señala esta autora, una medida de protección para el empresario y no para el consumidor, pues lo que se busca en realidad es darle tiempo al empresario.

Otra posible solución común la podemos hallar en el Marco Común de Referencia Europeo (DCFR, por sus siglas en inglés), un proyecto que tiene por objetivo la armonización del derecho contractual europeo²⁷⁰, en los Principios UNIDROIT y en los Principios De Derecho Europeo De Los Contratos (PECL) del profesor Ole Lando.

jurisprudencial poniendo su acento bien en la imprevisión e inevitabilidad, - fuerza mayor-, o en la previsión y evitabilidad, -caso fortuito- o por el contrario en que el acaecimiento se origine fuera de la empresa o círculo del deudor, - fuerza mayor-, o en el ámbito interno-caso fortuito”, véase STS, Sala 4ª, 1969/1997, de 22 de diciembre. *Recurso de casación para la unificación de doctrina. Reclamación de prestaciones*.

²⁶⁸ España. Real Decreto-ley 11/2020, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19, *Boletín Oficial del Estado*, 31 de marzo de 2020. Artículo 36.1.

²⁶⁹ TORRELLES-TOREA, E. (2021). “La resolución de los contratos por consumidores en tiempos de pandemia. Art. 36. 1 y 2 RD-ley 11/2020/”, *Revista de Derecho Civil*, Vol. 8, No. 2, p. 102. Disponible en: <https://www.nreg.es/ojs/index.php/RDC/article/view/635> (fecha de consulta: 2 de mayo de 2022).

²⁷⁰ Véase DE LA CUESTA-RUTE. J. (2011). “Sobre la unificación del Derecho privado patrimonial en Europa”, *Unificación del derecho patrimonial europeo marco común de referencia y derecho español* (Dir. VALPUESTA GASTAMINZA, E.), Ed.: Bosch, Barcelona, p. 23. Señala CAMPUZANO-DIAZ, B. (2004). “El plan de acción para un Derecho contractual europeo más coherente”, *Anuario Mexicano de Derecho Internacional*, p. 289-309. Disponible en: https://idus.us.es/bitstream/handle/11441/16281/1/file_1.pdf?sequence=1 (fecha de consulta: 23 de septiembre de 2021) que, el Marco Común de Referencia es fruto del Plan de Acción para un Derecho Contractual Europeo más Coherente, un proyecto que buscaba mejorar la situación del derecho contractual europeo.

El DCFR en el artículo III.-3:104²⁷¹ contempla la exoneración por imposibilidad del cumplimiento. En este sentido, el deudor queda exonerado del cumplimiento de una obligación cuando el incumplimiento está fuera de su control y no es razonable esperar que se hubiera evitado o superado. No obstante, el deudor tiene el deber que en un plazo razonable notifique el incumplimiento al acreedor, en caso contrario, la no notificación daría lugar a una indemnización por parte del deudor al acreedor, pero por los daños causados de no recibir tal notificación.

De manera similar, el artículo 8.108 PECL²⁷² y el artículo 7.1.7 de los Principios UNIDROIT²⁷³ siguen las líneas de DCFR en materia de incumplimiento. Ambos exoneran el cumplimiento por imposibilidad en el cumplimiento o excusan el incumplimiento, debido a un impedimento ajeno o fuera del control de las partes. Es decir, que la obligación no se pudo ejecutar por causas que están por fuera del control de los contratantes, porque fueron imprevistas o siendo previsible no pudieron ser superadas²⁷⁴. Si bien el deudor queda exonerado del cumplimiento, porque su incumplimiento es justificado, el acreedor aún conserva los remedios por incumplimiento, exceptuando el cumplimiento de la obligación y la indemnización de perjuicios, es decir, que el incumplimiento aun tendría consecuencias para el deudor. En el caso de los UNIDROIT,

²⁷¹ DELGADO- JEREZ, C. (2015). *Principios, definiciones y reglas de un Derecho Civil europeo: el Marco Común de Referencia (DCFR)*, Vol. 1, Boletín Oficial del Estado, p.136.

²⁷² Artículo 8:108: Exoneración por imposibilidad en el cumplimiento (1) Una parte queda liberada de su deber de cumplimiento si prueba que no puede proceder al cumplimiento de su obligación por un impedimento que queda fuera de su control y que no se puede pretender de manera razonable que hubiera debido tenerse en cuenta dicho impedimento en el momento de la conclusión del contrato o que la parte hubiera debido evitar o superar dicho impedimento o sus consecuencias. (2) Cuando el impedimento sea tan sólo temporal, la exoneración prevista en este artículo produce sus efectos durante el tiempo en el que persista el impedimento. Sin embargo, si el retraso se tradujera en un incumplimiento esencial, el acreedor puede tratarlo en tal sentido. (3) La parte que incumple debe asegurarse de que, en un plazo razonable desde que supo o hubiera debido enterarse de dichas circunstancias, la otra parte recibe una comunicación de la existencia del impedimento y de sus efectos sobre la capacidad de la parte para cumplir su obligación. La otra parte tiene derecho a una indemnización por daños y perjuicios por las pérdidas que pudieran resultar de no recibir esa comunicación. Traducido en “Principios De Derecho Europeo De Los Contratos”. (Sin fecha). Disponible en: <http://www.internationalcontracts.net/documentos-derecho-internacional/Principios-del-Derecho-Contractual-Europeo.pdf> (fecha de consulta: 12 de junio de 2021).

²⁷³ Artículo 7.1.7 (Fuerza mayor) (1) El incumplimiento de una parte se excusa si esa parte prueba que el incumplimiento fue debido a un impedimento ajeno a su control y que, al momento de celebrarse el contrato, no cabía razonablemente esperar, haberlo tenido en cuenta, o haber evitado o superado sus consecuencias. (2) Cuando el impedimento es sólo temporal, la excusa tiene efecto durante un período de tiempo que sea razonable en función del impacto del impedimento en el cumplimiento del contrato. (3) La parte incumplidora debe notificar a la otra parte acerca del impedimento y su impacto en su aptitud para cumplir. Si la notificación no es recibida por la otra parte en un plazo razonable a partir de que la parte incumplidora supo o debió saber del impedimento, esta parte será responsable de indemnizar los daños y perjuicios causados por la falta de recepción. (4) Nada de lo dispuesto en este artículo impide a una parte ejercitar el derecho a resolver el contrato, suspender su cumplimiento o a reclamar intereses por el dinero debido. Véase UNIDROIT. (2016). “Principios Unidroit Sobre Los Contratos Comerciales Internacionales 2016”. Disponible en: <https://www.unidroit.org/wp-content/uploads/2021/06/Unidroit-Principles-2016-Spanish-bl.pdf> (fecha de consulta: 12 de junio de 2021).

²⁷⁴ DELGADO- JEREZ, C. (2015). *Principios, definiciones... Op. Cit.*, p. 47.

señala el artículo 7.1.7 (4) que el acreedor puede resolver el contrato, suspender su cumplimiento o reclamar intereses por el dinero debido.

Evidentemente, esto sería problemático para los contratos inteligentes, puesto que al haber un error en el código es difícil establecer quién es la parte incumplida y aunque pudiera predicarse que el incumplimiento corresponde a uno de los contratantes, sería injusto, porque el deudor no queda exonerado de los efectos del incumplimiento, sino que estos quedan limitados. No obstante, los contratantes pueden incluir una cláusula que limite o excluya la responsabilidad por incumplimiento en caso de error de programación. Tanto los principios UNIDROIT²⁷⁵, como DCFR²⁷⁶ y PECL²⁷⁷ prevén que los contratantes puedan incluir este tipo de cláusulas siempre y cuando no sean contrario al principio de la buena fe o desleal.

Otra posible solución, sería aplicar la doctrina jurisprudencial de la cláusula *rebus sic stantibus*²⁷⁸ (estando así las cosas), que según sentencia del 17 de enero de 2003 del Tribunal Supremo, “trata de solucionar los problemas derivados de una alteración sobrevenida de la situación existente o circunstancias concurrentes al tiempo de la celebración del contrato, cuando la alteración sea tan acusada que aumente extraordinariamente la onerosidad o coste de las prestaciones de una de las partes o bien acabe frustrando el propio fin del contrato”²⁷⁹. Es decir, es una forma de reestablecer el equilibrio contractual.

Un remedio similar ha planteado GIANCASPRO para el derecho consuetudinario, quien ha sugerido que el contrato inteligente se ha frustrado “en virtud del hecho de que, sin culpa de ninguna de las partes, se ha vuelto imposible de realizar

²⁷⁵ ARTÍCULO 7.1.6 ARTÍCULO 7.1.6 (Cláusulas de exoneración) UNIDROIT Una cláusula que limite o excluya la responsabilidad de una parte por incumplimiento o que le permita ejecutar una prestación sustancialmente diversa de lo que la otra parte razonablemente espera, no puede ser invocada si fuere manifiestamente desleal hacerlo, teniendo en cuenta la finalidad del contrato.

²⁷⁶ III.-3:105 (...) (2) Si una cláusula excluye o limita un remedio por incumplimiento de una obligación, incluso aunque sea válida y tenga efectos de otro modo, no podrá invocarse, en virtud de las reglas relativas a cláusulas contractuales abusivas del Libro II, Capítulo 9, Sección 4, si el hacerlo fuera contrario al principio de buena fe contractual.

²⁷⁷ Artículo 8:109: Cláusulas de exclusión o de limitación de los medios de tutela Los medios de protección del crédito en caso de incumplimiento pueden excluirse o limitarse, salvo que resultase contrario a la buena fe alegar dicha exclusión o limitación.

²⁷⁸ Cláusula *hardship* en los contratos internacionales.

²⁷⁹ STS, Sala 1ª, 820/2013, de 17 de enero. *Contrato de compraventa de vivienda. Resolución de contrato. Rebus sic stantibus*

como se había previsto originalmente, por lo cual, el contrato se rescindirá y los contratantes quedarán liberados de su obligación”²⁸⁰.

Sin embargo, debido a las características de esta tecnología, en el supuesto que el contrato deba rescindirse o modificarse, existe el problema que el código siempre se ejecutará según lo programado, independientemente que si por la presencia de errores, es contrario a la intención de los contratantes, por lo que, en la práctica, dejar sin efecto o modificar un Smart Contracts es algo más complejo que en la contratación tradicional. Así que, si las partes no previeron una condicional que lo estipulara²⁸¹, que puede suceder muy a menudo, más que nada, porque se tendrían que anticipar todas las posibilidades de incumplimiento²⁸². Esta situación es difícil de alcanzar, pues hay factores externos que no se pueden prever, como, por ejemplo, un desastre natural o la pandemia de la COVID-19. Por ello, será necesario que por mutuo consentimiento las partes decidan revertir o modificar la operación, mediante la interacción con una nueva transacción, que invalide el contrato defectuoso, o mejor aún, que se redacte en el contrato la posibilidad de la intervención de un Tribunal que ordene revertir la ejecución del acuerdo o la posibilidad de que las partes renegocien las cláusulas del negocio jurídico.

A pesar de ello, como hemos mencionado anteriormente, si el contrato es víctima de un ataque, habrá consecuencias materiales que pueden llegar a ser irreversibles. En este sentido, una nueva transacción no podría devolver los fondos robados. Dicho sea de paso, la misma suerte seguirán los contratos que deban declararse nulos o anulables, pues se regirán por las leyes civiles y comerciales, pero en la práctica, se enfrentarán a los mismos obstáculos técnicos, lo que podría derivar en una pérdida de las garantías brindadas por el derecho contractual y al mismo tiempo el Smart Contracts carecería de una de sus ventajas más interesantes, la ejecución automática. Sin embargo, paradójicamente queda en evidencia que las soluciones a los

²⁸⁰ GIANCASPRO, M. (2017). "Is a 'smart contract' really ...", *cit.*, p. 829.

²⁸¹ Por ejemplo, las partes pueden codificar una cláusula de fuerza mayor que remita la llamada de un oráculo o juez, en caso que el cumplimiento se vea afectado, para que este resuelva la suerte que debe seguir el acuerdo.

²⁸² Las partes pueden incluir una cláusula de fuerza mayor que especifique qué eventos se pueden configurar como tal, sin embargo, es probable que esta cláusula no contenga todas las posibilidades, porque es difícil prever de antemano eventos futuros.

desafíos jurídicos de los contratos inteligentes se encuentran en la existencia de un contrato tradicional, que actúa de respaldo.

En resumen, es preciso que se desarrollen respuestas legales a estas cuestiones, que conlleven a una mejor adaptación del derecho contractual para el entorno de la contratación inteligente, porque si bien los Smart Contracts no lo reemplazaran, puede que algunas soluciones brindadas por este, tengan la necesidad de cambio, por resultar poco práctico o prohibitivamente alto para este tipo de contratación.

III.CONTRATOS INTELIGENTES EN UNA CADENA DE BLOQUES

1. Introducción

El diseño arquitectónico de las primeras cadenas de bloques, como Bitcoin, permiten ejecutar funciones simples de código, como transacciones de tipo moneda. Es decir, transferir dinero de una dirección A, a una dirección B. No obstante, las llamadas Blockchain de “segunda generación”²⁸³, como Ripple²⁸⁴, Ethereum²⁸⁵, Monax²⁸⁶, Rootstock (Rsk)²⁸⁷, Nxt²⁸⁸ y Corda²⁸⁹, entre otras, han permitido la realización de operaciones más complejas, gracias a que cuentan con capacidades de programación completas. De este grupo, la que más destaca por su popularidad es Ethereum, que admite

²⁸³ SWAN M. (2016). “Blockchain Temporality: Smart Contract Time Specifiability with Blocktime”, *Computer Science*, Vol. 9718, p. 191. Disponible en: https://doi.org/10.1007/978-3-319-42019-6_12 (fecha: de consulta 4 de agosto de 2020).

²⁸⁴ “RIPLE”. (Sin fecha). Disponible en: <https://ripple.com/> (fecha de consulta: 16 de junio de 2020).

²⁸⁵ “Ethereum”. (Sin fecha). Disponible en: <https://ethereum.org/es/> (fecha de consulta: 10 de junio de 2020).

²⁸⁶ Monax es una plataforma Blockchain para gestionar contratos inteligentes, herramientas y soluciones comerciales para empresas. Además, permite la integración con otras cadenas de bloques como Ethereum. Uno de sus principales objetivos es que los contratos sean legalmente vinculantes. Sobre el particular, puede consultarse la siguiente URL: “MONAX”. (Sin fecha). Disponible en: <https://monax.io/> (fecha de consulta: 20 de junio de 2020).

²⁸⁷ RootStock es una cadena de bloques de segunda generación cuyo objetivo es permitir la creación de contratos inteligentes dentro de Bitcoin, sin embargo, se ejecuta en paralelo a dicha Blockchain, por lo que es una SideChain (cadena lateral), véase “ROOTSTOCK”. (Sin fecha). Disponible en: <https://www.rsk.co/es/> (fecha de consulta: 16 de junio de 2020), “¿Qué es RootStock o RSK?”. (Sin fecha). Disponible en: <https://academy.bit2me.com/que-es-rootstock-rsk/> (fecha de consulta: 1 de julio de 2020).

²⁸⁸ Es una cadena de bloques 2.0, que soporta contratos inteligentes y cuyo protocolo de consenso es 100% Proof-of-Stake (prueba de participación), esto quiere decir que es íntegramente distribuido, al respecto véase “NXTER”. (Sin fecha). Disponible en: <https://www.nxter.org/understanding-nxt-cryptocurrency/> (fecha de consulta: 16 de junio de 2020).

²⁸⁹ Corda es una plataforma Blockchain de carácter privada con atributos de código abierto y orientada a buscar soluciones empresariales, sobre el particular véase “R3”. (Sin fecha). Disponible en: <https://www.r3.com/corda-platform/> (fecha de consulta: 16 de junio de 2020).

aplicaciones más allá de la transferencia de dinero²⁹⁰ y permite la ejecución automática de programas, popularmente conocidos como Smart Contracts²⁹¹, y que, en principio, no son acuerdos legales.

El funcionamiento de estos programas se basa en la lógica, si A, entonces B; lo que significa que si ocurre una condición se produce automáticamente una consecuencia²⁹². En otras palabras, ya no solo es la transferencia de una dirección A, a una dirección B; sino que dicha transferencia puede depender de una condición, por ejemplo, María recibirá una compensación por la cantidad de 100 euros si a María le cancelan su vuelo que tenía programada para el 30 de abril.

En esta sección, abordaremos el concepto de contratos inteligentes, sus características más sobresalientes y plantearemos la cuestión de si son o no inteligentes. Luego, describiremos a grandes rasgos cómo se desarrollan los Smart Contracts dentro de la plataforma de Ethereum y el funcionamiento de los mismos.

2. Concepto de contratos inteligentes

Intentar definir el término de contrato inteligente es una tarea difícil, por no decir, casi que imposible. A nivel doctrinal, nos encontramos con una multitud de definiciones que cuentan con una característica común definitoria, la ejecución automática sin

²⁹⁰ SERGEENKOV, A. (2020). "How Ethereum Works". Disponible en: <https://www.coindesk.com/learn/ethereum-101/how-ethereum-works> (fecha de consulta: 13 de julio de 2020).

²⁹¹ HILDENBRANDT, E., SAXENA, M., RODRIGUES, N., ZHU, X., DAIAN, P., GUTH, D., MOORE, B., PARK, D., ZHANG, Y., STEFANESCU, A. & ROSU, G. (2018). "KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine", *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*. Disponible en: <https://ieeexplore.ieee.org/document/8429306/authors#authors> (fecha de consulta: 14 de junio de 2020). Véase también "Ethereum". (Sin fecha). Disponible en: <https://ethereum.org/es/>

²⁹² BORSELLI, A. (2020). "Smart Contracts in Insurance: A Law and Futurology Perspective", *InsurTech: A Legal and Regulatory View*, (Dirs. MARANO, P. & NOUSSIA, K.), Ed.: Springer International Publishing. Disponible en: https://doi.org/10.1007/978-3-030-27386-6_5 (fecha de consulta: 16 de agosto de 2020).

intervención humana²⁹³; no obstante, aún no se ha logrado un consenso sobre un concepto universalmente aceptado²⁹⁴.

Antes de abordar estas consideraciones, es importante subrayar que el término contrato inteligente, en un contexto informático, difiere de lo que pueda considerarse como contrato en el ámbito legal. A nivel tecnológico, podría definirse como una pieza de *software* que se ejecuta de forma automática bajo ciertas condiciones, que opera de acuerdo a la lógica si/entonces, y que no necesariamente está destinado a crear efectos jurídicos. Es por esto, que la doctrina muy acertadamente, ha distinguido el contrato inteligente, del contrato legal inteligente (Smart Legal Contract), ya que este último, está diseñado para emular la lógica de las cláusulas jurídicas.

Aunque pueda parecer que son términos antagonistas, la realidad es que existe una correspondencia entre ambos, un contrato legal inteligente es un contrato escrito en lenguaje de programación, una pieza de código con trascendencia jurídica que se ejecuta dentro de los nodos de la red Blockchain. En consecuencia, todo contrato legal inteligente es un contrato inteligente, pero no todo contrato inteligente tiene que ser un contrato legal.

Teniendo en cuenta el carácter jurídico de nuestra investigación, una definición que consideramos completa, y tal como sus autores indican, es lo bastante amplia para abarcar tanto los contratos legales inteligentes, como los contratos inteligentes, es la de CLACK, BAKSHI Y BRAINE, quienes lo definen como “un acuerdo automatizable y exigible legalmente. Automatizable por ordenador, aunque algunas partes pueden requerir intervención y control humano. Se puede hacer cumplir ya sea mediante la

²⁹³ Véase EENMAA-DIMITRIEVA, H. & SCHMIDT-KESSEN, M.J. (2019). "Creating markets ...", *cit.*, p. 71, LEVY, K. (2017). "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law", *Engaging Science, Technology, and Society*, Vol 3. Disponible en: <https://estsjournal.org/article/view/107> (fecha de consulta: 8 de mayo de 2020). CHAMBER OF DIGITAL COMMERCE (2018) "Smart Contracts" Legal Primer Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable" Disponible en <https://bit.ly/2Zupmgm> (fecha de consulta 29 de febrero de 2019), RASKIN, M. (2017). "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review*, Vol. 304, p. 309. Disponible en: <http://dx.doi.org/10.2139/ssrn.2842258> (fecha de consulta: 2 de febrero de 2020). "Un contrato inteligente es un acuerdo cuya ejecución está automatizada". BOURQUE, S. & FUNG LING TSUI, S. (2014). "A Lawyer's Introduction to Smart Contracts", *Scientia Nobilitat: Reviewed Legal Studies*, Poland.

²⁹⁴ CIEPLAK, J. & LEEFATT, S. (2017). "Smart Contracts: A Smart Way ...", *cit.*, p. 427.

aplicación legal de derechos y obligaciones o mediante la ejecución de código informático que es a prueba de manipulaciones”²⁹⁵.

Esta definición es fundamental para el objetivo de nuestra investigación, ya que plantea que la ejecución del contrato inteligente se puede llevar a cabo, ya sea totalmente mediante el código de ordenador, o integrando las características de los contratos tradicionales (que suponen la intervención humana) con los contratos inteligente. De esta forma, se abarcan tanto las vías tradicionales, como las no tradicionales de ejecución contractual. Consideramos, que esta dualidad, será la forma en la que se desarrollarán en el futuro los contratos inteligentes que tengan un interés jurídico, puesto que hay términos y ficciones legales que no se podrán plasmar de forma eficiente en lenguaje de programación y necesariamente requerirán de la cognición humana.

Actualmente, se están desarrollando contratos con estas características, prueba de ello es la *integración dual* de los contratos inteligentes de MONAX o los del consorcio R3, que son una combinación de código de contrato inteligente y lenguaje natural, que se pueden hacer cumplir a través de un Tribunal. A todo esto, debemos sumarle que, tal y como advierte RASKIN, es poco probable una implementación pura y completa del contrato inteligente²⁹⁶, por lo menos no en un futuro cercano.

Debido a que los Smart Contracts se ejecutan en una Blockchain, posee unos atributos únicos, en contraste con los contratos tradicionales, a continuación, revisaremos de qué trata cada característica.

2.1 Inmutabilidad

El carácter inmutable significa que, si el acuerdo se registra en una cadena de bloques, este se ejecuta de manera descentralizada e independiente en la red de nodos, es decir, son contratos resistentes a la manipulación, por lo que ninguna de las partes puede

²⁹⁵ CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). "Smart Contract Templates: foundations, design landscape and research directions", p. 4. Disponible en: <https://arxiv.org/abs/1608.00771> (fecha de consulta: 10 de mayo de 2020).

²⁹⁶ RASKIN, M. (2017). "The Law and Legality...", *cit.*, p. 311.

falsificar o defraudar a la otra parte. El contrato inteligente se vuelve inmutable, al igual que la cadena de bloques donde se ejecuta²⁹⁷.

La rigidez de los Smart Contracts origina una serie de desafíos y tensiones con la naturaleza adaptable del derecho contractual tradicional, debido a que en algunos casos (o quizás en la mayoría), puede que esta inflexibilidad no sea apropiada, ya sea porque por mutuo consentimiento los contratantes decidan cambiar los términos contractuales, porque se necesite corregir un error en el código, o porque es necesaria la intervención judicial en caso de una disputa.

La naturaleza inmutable de los Smart Contracts limita el ejercicio de una multiplicidad de derechos y principios consagrados en las leyes contractuales, lo que supone un límite para su aplicación, especialmente, si consideramos el carácter dinámico de las relaciones comerciales. Sin embargo, si la inmutabilidad de Blockchain implica que un contrato es inalterable en cualquier circunstancia. Resulta evidente que la bifurcación dura adoptada por la mayoría de los nodos de Ethereum, como consecuencia del ataque a la DAO, pone en duda la integridad de esta característica, más aún, si se ha visto que los equipos de desarrollos de varios proyectos de Ofertas Iniciales de criptomonedas, pueden modificar unilateralmente los tokens adquiridos por los inversores²⁹⁸, ya que el código del contrato inteligente que controla la oferta, puede ser programado para permitir tal modificación.

2.2 Autoejecutable

El carácter autoejecutable significa que la ejecución del contrato se realiza de forma automática, sin intervención humana, una vez se cumplen las condiciones pre codificadas. Por ejemplo, imagine que la compañía de seguros Bit le pagará una compensación a Juan de cien euros, si su vuelo se retrasa por más de quince minutos, o realizar un determinado desembolso de dinero en una fecha específica. La ejecución automática conlleva a que sea el propio algoritmo el que verifique de forma determinista

²⁹⁷ LOW, K. & MIK, E. (2019). "Pause the Blockchain Legal ...", *cit.*, p. 170

²⁹⁸ COHNEY, S., HOFFMAN, D., SKLAROFF, J. & WISHNICK, D. (2019). "Coin-Operated ...", *cit.* p. 634.

o mediante la entrada de una fuente externa (oráculo), si se han cumplido las condiciones que desencadenan el resultado preestablecido.

Lógicamente, esta particularidad dota a la transacción de seguridad, ya que el cumplimiento no depende de las partes, sino del código. No obstante, en muchas ocasiones puede ocurrir que los contratantes deseen detener el cumplimiento, o que surja una disputa y un juez ordene su suspensión. Sin embargo, esta característica genera un enfrentamiento con el derecho contractual, puesto que en principio “una orden judicial no puede deshacer los resultados de un contrato ejecutado”²⁹⁹. De tal manera que esta no tendría ningún efecto práctico³⁰⁰, ya que el contrato se ejecutará de forma determinista, aunque como tendremos ocasión de ver más adelante, existen mecanismos técnicos que pueden revertir, si bien de forma limitada, los efectos materiales de un Smart contract ejecutado.

2.3 Seudónimo

Muchas veces se piensa que las transacciones que se realizan en Blockchain son anónimas, pero esto no es del todo cierto, porque si bien las personas no se identifican por su nombre real, lo hacen mediante claves públicas (o direcciones), las cuales están expuestas en la cadena de bloques³⁰¹; lo que las convierte en seudónimas. Por tanto, como los contratos inteligentes se ejecutan a través de los nodos de la red Blockchain, las claves criptográficas públicas de los contratantes son visibles por todos³⁰², evidentemente, esto provoca un problema con la privacidad de los datos de un contrato, máxime cuando varios estudios³⁰³ de rastreos de criptomonedas han demostrado que es posible la identificación del titular de las claves.

²⁹⁹ WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *cit.*, p. 121.

³⁰⁰ DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under ...", *cit.*, p. 77., "Contracts ex machina", *cit.*, p. 161.

³⁰¹ KOSBA, A., MILLER, A., SHI, E., WEN, Z. PAPAMANTHOU, C. (2016). "The blockchain model of cryptography and privacy-preserving smart contracts", *2016 IEEE symposium on security and privacy*, p. 839. Disponible en: <https://ieeexplore.ieee.org/document/7546538> (fecha de consulta: 12 de abril de 2020).

³⁰² DRESCHER, D. (2017). *Blockchain Basics A Non-Technical Introduction in 25 Steps*, Apress, p. 101. Berkeley, CA.

³⁰³ Véase a FENG, Q., HE, D., ZEADALLY, S., KHAN, M.K. & KUMAR, N. (2019) "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, Vol. 126, p. 45-58. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S1084804518303485#bib48> (fecha de consulta 15 de abril de 2020), HEAVEN, D. (2018). "Así trabajan los detectives de robos de criptomonedas en 'blockchain'", *Technology Review*. Disponible en: <https://www.technologyreview.es/s/10171/asi-trabajan-los-detectives-de-robos-de->

2.4 No son tan inteligentes

Una de las grandes críticas que ha recibido el término de contrato inteligente, es si realmente se puede denominar o no inteligente. Es muy común la expresión: no son inteligentes, ni contratos³⁰⁴. La génesis de la discusión se genera porque las transacciones se ejecutan de forma automática, cuando se cumplen las condiciones previamente programadas, sin entrar a valorar otros factores³⁰⁵.

En la actualidad los Smart Contracts son secuencias de códigos estáticos que se ejecutan de forma automática sin razonar, por lo que el término contrato inteligente es un nombre “impreciso para un *software* que se ejecuta mecánicamente”³⁰⁶. La condicional, si/entonces, produce de forma determinista una consecuencia mecanizada. Dicho de otra manera, los contratos inteligentes no tienen la capacidad de “pensar”, solo siguen de forma ciega instrucciones preprogramadas. El diseño fijo e inmutable impide cualquier flexibilidad, por lo que no se pueden adaptar a cualquier cambio sobrevenido.

La doctrina ha sugerido llamarlos de otra forma, como, por ejemplo, *Bot Contracts*³⁰⁷ (contrato de robots), pues esta denominación engloba más la naturaleza estática de estos acuerdos, o como *mecanismos*, porque harán exactamente lo programado en su código³⁰⁸. Incluso, el mismo VITALIK BUTERIN, cofundador de Ethereum, se lamentó en su cuenta personal de Twitter haberle puesto este nombre, ya que hubiese sido

criptomonedas-en-blockchain (fecha de consulta 22 de abril de 2020) y SIMONITE, T. (2013). “Las identidades de los usuarios de Bitcoin podrían salir al descubierto”, *Technology Review*. Disponible en: <https://www.technologyreview.es/s/3757/las-identidades-de-los-usuarios-de-bitcoin-podrian-salir-al-descubierto>. (fecha de consulta 22 de abril de 2020).

³⁰⁴ CHAMBER OF DIGITAL COMMERCE. (2018). “Smart Contracts” Legal Primer Why ...”, *cit.*, p. 1. Disponible en: <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> (fecha de consulta: 29 de febrero de 2019).

³⁰⁵ MCJOHN, S. & MCJOHN, I. (2016). “The Commercial Law of Bitcoin and Blockchain Transactions”, *Uniform Commercial Code Law Journal*, Vol. 47, No. 2. pp. 187-222. Disponible en: <https://ssrn.com/abstract=2874463> como se citó en: LEGERÉN-MOLINA, A. (2018). “Los contratos inteligentes...”, *cit.*, p. 205.

³⁰⁶ En efecto, la Cámara de Comercio Digital lo ha catalogado como un término imperfecto, véase CHAMBER OF DIGITAL COMMERCE. (2018). “Smart Contracts” Legal Primer Why ...”, *cit.*, p. 1. Véase también LIPSHAW, J.M. (2019). “The Persistence of “Dumb” Contracts”, *Stanford Journal of Blockchain Law & Policy*, Vol. 2, No. 1. Disponible en: <https://stanford-jblp.pubpub.org/pub/persistence-dumb-contracts/release/1> (fecha de consulta: 25 de marzo de 2020) y DUROVIC, M. & JANSSEN, A. (2019)., *cit.*, p. 74.

³⁰⁷ GERHARDT, D. & THAW, D. (2020). “Bot contracts”, *Arizona Law Review*, p. 877. Disponible en: <https://ssrn.com/abstract=3533517> (fecha de consulta: 18 de agosto de 2020).

³⁰⁸ FELTEN, E. (2017). “Smart Contracts: Neither Smart nor Contracts?”. Disponible en: <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/> (fecha de consulta: 25 de junio de 2020).

mejor un nombre más aburrido y técnico como "*Persistent scripts*"³⁰⁹, el cual no ocasionaría tanta confusión.

La realidad no es precisa como un lenguaje de programación, muchas relaciones jurídicas no pueden enmarcarse en la lógica Si/entonces, ni tampoco pueden describirse de forma objetiva. Por ejemplo, un ordenador no puede determinar si uno de los contratantes ha actuado de buena fe, de modo que se necesita una valoración subjetiva, que, hasta el día de hoy, a pesar de los avances de la inteligencia artificial, un *software* no es capaz de evaluar o determinar. Por consiguiente, algunos contratos inteligentes requerirán que una parte de su desempeño se realice fuera de Blockchain, ya sea porque no se puede automatizar, o porque necesiten de la intervención de un tribunal para la resolución de disputas.

Ello no quiere decir que le estamos restando importancia a los contratos inteligentes, ni que la automatización pueda introducir consecuencias deseables. Todo lo contrario, hay buenas razones para creer en su potencial disruptivo y su capacidad de ofrecer confianza, eliminar la incertidumbre y dotar en términos de eficiencia los acuerdos cuyas cláusulas sean susceptibles de automatización. No obstante, la inteligencia se refiere a su capacidad de automatizar ciertas acciones y no al sentido literal del significado.

3. Ethereum

Ethereum, es una plataforma digital pública, descentralizada y de código abierto³¹⁰. Actualmente, es el segundo desarrollo Blockchain más grande del mundo. Posee una criptomoneda nativa llamada ETHER y cuenta con un lenguaje de programación Turing completo³¹¹. Es decir, que tiene el poder computacional igual al de la máquina de Turing universal, un concepto teórico ideado por ALAN TURING, que se

³⁰⁹ “@VitalikButerin”. (2018). Disponible en: <https://twitter.com/VitalikButerin/status/1051160932699770882> (fecha de consulta: 29 de junio de 2020).

³¹⁰ Esto quiere decir que es un tipo de desarrollo de *software* en el que cualquier persona puede participar. “Ethereum”. Disponible en: <https://ethereum.org/es/> (fecha de consulta: 10 de junio de 2020). Véase MALDONADO, J. (2020). “¿Qué es la Ethereum Virtual Machine (EVM)? La máquina virtual de Ethereum”. Disponible en: <https://es.cointelegraph.com/explained/what-is-the-ethereum-virtual-machine-evm-the-ethereum-virtual-machine> (fecha de consulta: 16 de junio de 2020).

³¹¹ ETHEREUM. (2020). “[Spanish] White Paper Ethereum”. Disponible en: <https://github.com/ethereum/wiki/wiki/%5BSpanish%5D-White-Paper.md> (fecha de consulta: 10 de junio de 2020).

refiere a una máquina que es capaz de ejecutar cualquier algoritmo. Dicho de otra, es una cadena de bloques programable, lo que les permite a los desarrolladores ejecutar y crear aplicaciones descentralizadas (DApps) que se ejecutan automáticamente y, por lo tanto, puede resolver cualquier problema computacional. Ello supone que, puede hacer lo que otro programa de ordenador puede hacer³¹², como, por ejemplo, controlar la temperatura de un local o implementar reglas complejas como los bucles.

Un bucle, en programación, es una instrucción que se ejecuta repetidamente hasta que la condición asignada no se cumpla, es decir, son tareas repetitivas hechas por el código³¹³. Por ejemplo, imagine que Marcos debe pagarle a María, Juan y Pedro una paga de cien euros, en vez de escribir el mismo código tres veces para que se ejecute el contrato, se pone en un bucle para que este se ejecute tres veces.

Ethereum explica que para evitar que se genere un bucle infinito (un Smart Contracts que se ejecuta indefinidamente) e impedir que la red pueda ser colapsada³¹⁴, como consecuencia de la integridad de Turing completo del lenguaje de programación, y al hecho de que cada Smart Contracts se ejecuta a través de todos los nodos de la cadena de bloques³¹⁵, se implementó una medida en la cual todas las operaciones que se hagan en la Máquina Virtual de Ethereum ³¹⁶ (EVM, por sus siglas en inglés, *Ethereum Virtual Machine*) tienen un costo asociado a dicho calculo computacional.

³¹² KAAL, W.A. & CALCATERRA, C. (2018). "Crypto Transaction Dispute Resolution", *the business lawyer*, p. 5. Disponible en: <http://dx.doi.org/10.2139/ssrn.2992962> (fecha de consulta: 20 de agosto de 2019).

³¹³ "Solidity todos los recursos sobre el lenguaje de programación de los smart contracts". (Sin fecha). Disponible en: <https://www.miethereum.com/smart-contracts/solidity/> (fecha de consulta: 10 de junio de 2020).

³¹⁴ Por ejemplo, un atacante podría realizar contratos que incluyan muchas operaciones y de esta forma ralentizar la red. Ver HOLLANDER, L. (2019). "The Ethereum Virtual Machine — How does it work?". Disponible en: <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e> (fecha de consulta: 25 de junio de 2020). Esto sería un tipo de ataque de denegación de servicio, también conocido como DDoS. un ataque que ralentiza el servidor como consecuencia de muchas peticiones, superando el límite de la capacidad de la red.

³¹⁵ PETERS, G.W. & PANAYI, E. (2016). "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money", *Banking Beyond Banks and Money A Guide to Banking Services in the Twenty-First Century*, (Dir. TASCA, P., TOMASO, A., PELIZZON, L. & PERONY, N.), Ed.: Springer, Cham., p. 245.

³¹⁶ La máquina virtual de Ethereum es un *software* cuya función es la de imitar un ordenador real.

El pago se hace en unidades Gas³¹⁷, se compra con Ether (*ETH*), que se paga con dinero del mundo real³¹⁸. La tarifa la paga por adelantado el remitente de cada transacción a los mineros³¹⁹. Su valor depende de la complejidad de la operación y se agota a medida que se va ejecutando. La implementación del Gas, no solo evita que el sistema pueda ser víctima de un ataque, sino que incentiva el trabajo de los validadores, quienes son los que se encargan del correcto funcionamiento de la Red. Esto se traduce en que todo contrato inteligente para ser implementado, almacenado y ejecutado dentro de la Ethereum, debe pagar un precio prohibitivamente alto. Un Smart contract muy básico cuesta alrededor de 500 USD, mientras que uno complejo, que ocupe mucho espacio de almacenamiento, puede llegar a costar más de 80 millones de dólares³²⁰. Ello se debe, entre otras cosas, al aumento de precio que ha experimentado el Ether en 2021 y a los límites de almacenamiento y procesamiento que tiene dicha cadena de bloques por diseño³²¹.

Como se mencionó anteriormente, los programas que se ejecutan en Ethereum, están escritos en lenguajes de programación de alto nivel ³²², por ejemplo, Bamboo³²³, Vyper³²⁴ o Solidity³²⁵. De estos el más utilizado y popular para escribir Smart Contracts

³¹⁷ El gas es el pago por los recursos informáticos necesarios para los pasos informáticos en los contratos inteligentes, y los mineros que construyen los bloques y ofrecen sus recursos informáticos reciben el pago. Véase PARK, J., LEE, D. & IN, H. (2017) "Saving deployment costs of smart contracts by eliminating gas-wasteful patterns", *International Journal of Grid and Distributed Computing*, Vol. 10, no 12, p. 54. Disponible en: <http://dx.doi.org/10.14257/ijgdc.2017.10.12.06> (fecha de consulta: 16 de junio de 2020). Para entender detalladamente cómo funciona el Gas véase, "What Is Gas?". (2020). Disponible en: <https://support.mycrypto.com/general-knowledge/ethereum-blockchain/what-is-gas> (fecha de consulta: 25 de junio de 2020).

³¹⁸ PARK, J., LEE, D. & IN, H. (2017) "Saving...", *cit.*, p. 53.

³¹⁹ Al respecto HILDENBRANDT, E., SAXENA, M., RODRIGUES, N., ZHU, X., DAIAN, P., GUTH, D., MOORE, B., PARK, D., ZHANG, Y., STEFANESCU, A. & ROSU, G. (2018). "KEVM: A Complete Formal Semantics ...", *cit.*, p. 206, sostienen que, "El programa de tarifas para la ejecución está totalmente acordado por la red, y cada transacción especifica una cantidad máxima de gas que está dispuesto a usar, así como su tipo de cambio entre Ether y gas. Si una transacción se queda sin gasolina durante la ejecución, se cancela, sus actualizaciones de estado se revierten y los mineros se quedan con las tarifas de gas de la transacción."

³²⁰ Precios de octubre de 2021. Hay que tener en cuenta las fluctuaciones abruptas que puede experimentar en un día el mercado de las criptomonedas.

³²¹ LASTNAME, E. (2021). "How much does it cost to deploy a smart contract on Ethereum?" Disponible en: <https://medium.com/the-capital/how-much-does-it-cost-to-deploy-a-smart-contract-on-ethereum-11bcd64da1> (fecha de consulta: 1 de noviembre de 2021)

³²² HARZ, D. & KNOTTENBELT, W. (2018). "Towards Safer Smart Contracts: A Survey of Languages and Verification Methods". Disponible en: <https://arxiv.org/abs/1809.09805> (fecha de consulta: 14 de junio de 2020).

³²³ Puede consultar más información en "Bamboo: a language for morphing smart contracts". (Sin fecha). Disponible en: <https://github.com/pirapira/bamboo> (fecha de consulta: 11 de junio de 2020).

³²⁴ "Vyper". (Sin fecha) Disponible en: <https://vyper.readthedocs.io/en/stable/> (fecha de consulta: 11 de junio de 2020).

³²⁵ Puede consultar más información en "Solidity". (Sin fecha). <https://docs.soliditylang.org/en/v0.8.17/> (fecha de consulta: 11 de junio de 2020).

es el último citado (Solidity)³²⁶, que consiste en un lenguaje, orientado a datos e inspirado en C++, Python y Javascript³²⁷.

Solidity, tiene como objetivo la integración con la EVM, sin embargo, no puede ser directamente ejecutado en esta, por lo que el código de Solidity se transforma a *OP_CODES*³²⁸ y luego a *Bytecodes*. Dicho de otra manera; el código se compila o traduce³²⁹ a *Bytecodes* para que pueda ser comprendido y ejecutado en la EVM³³⁰ (en código binario que es el que la Máquina Virtual puede entender)³³¹. Esta funcionalidad es la que posibilita el desarrollo de programas que se ejecuten en la red Blockchain.

En resumen, la Máquina Virtual (EVM) es el núcleo de Ethereum, pues no solo es el entorno de ejecución de los contratos inteligentes, sino que, es un *software* que emula todas las funciones de un ordenador real, y le otorga seguridad a la cadena de bloques, ya que sirve como capa de abstracción, es decir, que está completamente aislada, de tal manera que el código que se ejecuta en la EVM, no tiene acceso a la red u otros procesos³³².

4. Funcionamiento de los contratos inteligentes

Si bien Blockchain ha proporcionado la tecnología necesaria para el desarrollo de los Smart Contracts³³³, lo cierto es que su funcionamiento no depende necesariamente de

³²⁶ Véase “Ethereum”. Disponible en: <https://ethereum.org/es/> (fecha de consulta: 10 de junio de 2020).

³²⁷ “Solidity”. (Sin fecha). <https://docs.soliditylang.org/en/v0.8.17/> (fecha de consulta: 11 de junio de 2020).

³²⁸ Al respecto en “¿Qué es un OP_CODE?”. (Sin fecha). Disponible en: <https://academy.bit2me.com/que-es-un-op-code/> (fecha de consulta: 16 de junio de 2020) se señala que, “También conocido como código de operación, son las instrucciones e indicaciones que se utilizan para la programación de (...) máquinas virtuales”.

³²⁹ Traducir un código de programación a código ejecutable por la máquina.

³³⁰ PARIZI, M., AMRITRAJ & DEGHANTANHA, A. (2018). “Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security”, *Computer Science*, Vol. 10974. p. 77. Disponible en: https://doi.org/10.1007/978-3-319-94478-4_6 (fecha de consulta 4 de agosto de 2020).

³³¹ Al respecto DEWEY, J. (2016). “What if we developed legal contracts like we developed software applications?” Disponible en: <https://medium.com/@Consensys/what-if-we-developed-legal-contracts-like-we-developed-software-applications-1b5bc8fbb915> (fecha de consulta 21 de julio de 2020), señala que, “las computadoras comprenden solo una serie de unos y ceros o dos estados, “encendido” y “apagado””.

³³² “The Ethereum Virtual Machine”? (Sin fecha). Disponible en: <https://docs.soliditylang.org/en/v0.6.11/introduction-to-smart-contracts.html#the-ethereum-virtual-machine> (fecha de consulta: 10 de junio de 2020).

³³³ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 73.

una cadena de bloques, ni su uso está supeditado a una criptomoneda³³⁴. Por ejemplo, los contratos ejecutados por agentes electrónico³³⁵, EDI o Ricardian Contracts, no requieren del uso de esta tecnología, como acertadamente señalan los profesores ARDOLESI y DAVOLA, para quienes Blockchain “es solo una de las posibles herramientas para su implementación”³³⁶.

No obstante, su aplicación en una Blockchain es la única tecnología que puede permitir la ejecución automática de transacciones dinerarias, sin necesidad de la intervención humana, (hecho que no ocurre con los sistemas de pagos tradicionales³³⁷) asegurando la integridad de su código y garantizando la ejecución descentralizada³³⁸.

Los Smart Contracts se desarrollan mediante scripts (códigos informáticos)³³⁹ alojados en Blockchain que representan instrucciones escritas en lenguaje de programación³⁴⁰. Dichos programas ejecutan de forma automática determinadas tareas según las condiciones programadas en su código. Este funcionamiento responde a un concepto matemático conocido como Lógica Booleana³⁴¹, lo que significa que las cláusulas “han de tener la estructura *if/then/else*: si se cumple esta circunstancia (*if*), entonces se ejecuta esta acción (*then*); de no cumplirse, se ejecuta otra acción también

³³⁴ RÜHL, G. (2020). "Smart (Legal) "Contracts, or: Which (Contract) Law for Smart Contracts?", *Blockchain, Law and Governance*, (Drs. CAPPIELLO B. & CARULLO G.) Ed.: Springer International Publishing, Cham, p. 164. Véase también DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under ...", *cit.*, p. 64.

³³⁵ Véase DELL'ERBA, M. (2019). "Demystifying Technology...", *cit.*, p. 12 y CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). "Smart Contract Templates: foundations...", *cit.*, p. 3.

³³⁶ PARDOLESI, R. & DAVOLA, A. (2019). "What is wrong in ...", *cit.*, p. 8.

³³⁷ ECHEBARRÍA SÁENZ, M. (2017). "Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain", *Revista de estudios europeos*, No. 70, pp. 74-75. Disponible en <http://uvadoc.uva.es/handle/10324/28434> (fecha de consulta 16 de abril de 2019). Según TAKAHASHI, K. (2018). "Blockchain and Smart Contract...", *cit.*, p. 5, un Smart Contracts no puede realizar pagos en dinero fiat a menos que los bancos centrales emitan monedas del curso legal en una cadena de bloques.

³³⁸ LOW, K. & MIK, E. (2019). "Pause the Blockchain Legal ...", *cit.*, p. 170.

³³⁹ "Smart Contracts: ¿Qué son, ¿cómo funcionan y qué aportan?". (Sin fecha). Disponible en: <https://academy.bit2me.com/que-son-los-smart-contracts/> (fecha de consulta: 10 de junio de 2020).

³⁴⁰ "Monax legacy content- What are Smart Contracts?". (Sin fecha). Disponible en: https://github.com/monax/legacy-content/blob/master/learn/smart_contracts.md (fecha de consulta: 10 de junio de 2020).

³⁴¹ OTERO, L. (2019). "Análisis jurídico de los smart contract". Disponible en: https://www.legaltoday.com/legaltech/novedades-legaltech/analisis-juridico-de-los-smart-contract-2019-05-23/#_ftn2 (fecha de consulta: 15 de mayo de 2020). La lógica Booleana es una estructura algebraica desarrollada por el matemático inglés George Boole. Al respecto explica ISDA & LINKLATERS. (2017). "Whitepaper Smart Contracts ...", *cit.*, p. 11, que “esta lógica solo trabaja con dos variables: “1” y “0” o “verdadero” y “falso”. “Forma la base de las computadoras modernas y de los lenguajes de programación de computadoras. En los lenguajes de programación de ordenadores, las declaraciones condicionales realizan diferentes cálculos o acciones dependiendo de si una condición booleana es verdadera o falsa. Esto a menudo se expresa en forma de declaraciones if - then - else, es decir, si se cumple la condición booleana, entonces [hacer algo] más [hacer otra cosa]”.

prevista (*else*)”³⁴². Dicho de otra forma, la lógica booleana es un sistema binario que “solo admite uno de dos valores de entradas y salidas, sí/no, verdadero/falso, 0/1”³⁴³, es decir, algo es “falso” o “verdadero” es “0” o “1”.

Las partes, tras firmar el contrato mediante claves criptográficas³⁴⁴ dotan a la transacción de seguridad y confianza. Una vez se cumplen las condiciones programadas, el acuerdo se ejecuta de forma independiente a través de todos los nodos de la red Blockchain³⁴⁵, quedando los datos almacenados en la cadena de bloques. Por esta razón, no son susceptibles de automatización las cláusulas de carácter ambiguo, en virtud de que, los lenguajes de programación no pueden tener varios significados al mismo tiempo, lo que elimina los términos vagos e indeterminados en la contratación. Lógicamente, esta característica plantea una serie de dudas y cuestiones legales.

No obstante, en el área de la computación cuántica, el desarrollo de los *Cúbit*³⁴⁶, en contraste con la informática tradicional, que solo puede estar en un solo estado a la vez, “0” o “1”, encendido o apagado, falso o verdadero. Los bits cuánticos tienen la capacidad de superposición, lo que les permite codificar “1” y “0” al mismo tiempo. Ello implica, que se pueden realizar más cálculos simultáneamente³⁴⁷. Quizás por esto, este tipo de tecnologías son capaces de abrir posibilidades a la codificación de cláusulas ambiguas, pero su desarrollo aún puede tardar muchísimos años en materializarse.

Para el adecuado funcionamiento de un contrato inteligente, hace falta dos elementos de suma importancia: multifirma (*Multisig*) y oráculos³⁴⁸.

³⁴² LEGERÉN-MOLINA A. (2019). "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de Blockchain", *Revista de Derecho Civil*, Vol. 6, No. 1, p. 223. Disponible en: <https://www.nreg.es/ojs/index.php/RDC/article/view/356> (fecha de consulta: 14 de abril de 2020).

³⁴³ ULPGC. (2015). “De Boole a Google: la lógica booleana en la vida cotidiana”. Disponible en: https://biblioteca.ulpgc.es/noticia_bicentenario_george_boole (fecha de consulta: 12 de febrero de 2021).

³⁴⁴ O'SHIELDS, R. (2017). "Smart Contracts...", *cit.*, p. 179.

³⁴⁵ PETERS, G.W. & PANAYI, E. (2016). “Understanding Modern Banking ...”, *cit.*, p. 245.

³⁴⁶ Son también denominados Bits cuánticos, es un concepto análogo cuántico a los bits en la computación tradicional.

³⁴⁷ BOUGUERA, A. (2019). “How Will Quantum Computing Affect Blockchain?” Disponible en: <https://consensus.net/blog/blockchain-development/how-will-quantum-supremacy-affect-blockchain/> (fecha de consulta: 1 de octubre de 2020). Véase también VANEGAS – GOMEZ, A. (20116). “El camino hacia el ordenador cuántico: qubits y qudits”. Disponible en: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/el-camino-hacia-el-ordenador-cuatico-qubits-y-qudits/> (fecha de consulta: 1 de octubre de 2020).

³⁴⁸ DELL'ERBA, M. (2019). “Demystifying Technology...”, *cit.*, p.16.

4.1 Multifirma

Es una de las características más interesantes de los contratos inteligentes. Este elemento dota de seguridad las transacciones, puesto que requiere que dos o más partes la aprueben para que el contrato pueda seguir siendo ejecutado. Dicho de otra forma, es necesario dos de las tres claves para que el contrato pueda avanzar (una está en posesión de cada parte y la restante está en manos de un tercero); de tal manera que el Smart Contract está controlado conjuntamente por dos o más personas, impidiendo que una sola tenga el control absoluto.

Este sistema resulta de gran utilidad para la resolución de disputas, por ejemplo, imagine que Ana le compra a Pedro un producto, el contrato inteligente mantiene los fondos retenidos hasta que Ana no reciba el producto en perfectas condiciones. En caso de una controversia acerca de la idoneidad del bien, la firma del tercero, es la que resolverá la disputa y determinará si se liberan o no los fondos. También, se puede dar el caso, que no surja ningún conflicto, tanto María como Pedro pueden firmar la transacción si el producto se recibe en perfecto estado, o porque quieren rescindir mutuamente el contrato.

4.2 Oráculo

Las cadenas de bloques no están conectadas a internet³⁴⁹, por esta razón no pueden recibir entradas del mundo exterior, de manera que un contrato inteligente que necesite actualizar un precio o que requiera de algún tipo de información que ocurra fuera de la cadena, precisa que un proveedor de servicios suministre dicha información. Este proveedor de información, se conoce como oráculo, y permite monitorear eventos que suceden por fuera de Blockchain y, por lo tanto, actualizar el estado de los contratos. Es una fuente externa que posibilita a los Smart Contracts interactuar con el mundo real³⁵⁰.

Para entender su funcionamiento, es esencial repasar brevemente cómo opera una transacción. Las transacciones trabajan con criptografía asimétrica (clave pública o

³⁴⁹ DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under ...", *cit.*, p. 66.

³⁵⁰ BARTOLETTI, M. & POMPIANU, L. (2017.) "An empirical analysis of smart contracts: platforms, applications", p. 10. Disponible en: <https://arxiv.org/pdf/1703.06322.pdf%20pp%2010.pdf> (fecha de consulta: 15 de mayo de 2020).

direcciones)³⁵¹; lo que significa que hay dos claves: una pública y una privada, las cuales están vinculadas entre sí. La clave pública es visible “públicamente” y los datos cifrados en ella únicamente pueden ser descifrados por la clave privada³⁵². Es decir, cuando se transfieren Tokens de una cuenta B a una cuenta C, solamente la clave privada de la cuenta C puede acceder a ellos. Cada transacción tiene un *script* que estipula que los tokens son pagaderos a la clave privada que desbloquee la clave pública³⁵³. No obstante, muchas veces el *script* de desbloqueo de los Tokens está supeditado a la ocurrencia de una condición que tiene lugar fuera de la cadena de bloques, por lo que, se hace necesario el papel de un tercero u oráculo, quien luego de verificar la ocurrencia del evento, firmará con su clave privada para desbloquear el *script* que controla los Tokens³⁵⁴.

En definitiva, los oráculos son un puente entre el mundo físico y virtual³⁵⁵, un intermediario centralizado³⁵⁶ y no confiable cien por ciento; en el sentido que la información que recolectan la obtienen de proveedores comerciales externos³⁵⁷. De tal forma que la información comunicada puede no ser auténtica, como consecuencia de algún tipo de ataque, ya que las propiedades que hacen a las cadenas de bloques seguras, no son extrapolables o no son compartidas a los oráculos.

Estas características introducen la presencia de intermediarios, socavan la descentralización y la falta de confianza en terceros, rasgos fundamentales de las bases ideológicas de esta tecnología. Lógicamente, ello ha generado que los oráculos sean objetos de múltiples críticas, pues de nada sirve que las cadenas de bloques sean seguras y “sin confianza”, si los contratos inteligentes precisan de información brindada por terceros que son sin confianza y cuya autenticidad no se puede verificar.

³⁵¹ Se aborda con más detalle esta cuestión en el capítulo quinto, título II, apartado 2 de la presente obra.

³⁵² DRESCHER, D. (2017). *Blockchain Basics A Non-Technical ...*, Op. Cit., p. 93.

³⁵³ MIK, E. (2017). “Smart contracts: Terminology...”, cit., p. 22.

³⁵⁴ MIK, E. (2017). “Smart contracts: Terminology...”, cit., p. 22.

³⁵⁵ CANNARSA, M. (2019). “Contract Interpretation” *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 102-106.

³⁵⁶ Advierte ORCUTT, M. (2019). “Cómo asegurar la información que gobierna los contratos inteligentes”, *technology review*. Disponible en: <https://www.technologyreview.es/s/10757/como-asegurar-la-informacion-que-gobierna-los-contratos-inteligentes> (fecha de consulta: 19 de noviembre de 2020), que, “Los servicios de oráculos actuales están demasiado de centralizados” ello genera que se conviertan en fuentes de errores sujetas a la manipulación externa.

³⁵⁷ GERHARDT, D. & THAW, D. (2020). “Bot...”, cit., pp. 890-891.

IV. LENGUAJE DE PROGRAMACIÓN Y LENGUAJE NATURAL

1. De la ambigüedad y otros demonios

Parte del entusiasmo que ha suscitado la implementación de los contratos inteligentes se debe a que eliminan la ambigüedad en la contratación. A menudo se comparan las desventajas de los contratos tradicionales, redactados en lenguaje natural, que tiende a estar plagado de ambigüedades y de términos inexactos, frente a los beneficios de los contratos inteligentes, escritos en lenguaje de código que al ser binario resuelven el problema de la ambigüedad³⁵⁸ lo que los hace más seguro³⁵⁹ y más eficientes, ya que el riesgo de litigio es casi nulo³⁶⁰.

Los informáticos tienden a pensar, quizás por analogía, porque la ambigüedad en lenguajes de programación es considerada como un anatema³⁶¹, que la vaguedad en la contratación es indeseable y que, por lo tanto, es un problema que necesita una solución³⁶². Lo cierto es que un “contrato no es un intercambio entre máquinas, si no una práctica social entre personas, por lo que los resultados a menudo son completamente demostrables en matemáticas, pero inútiles como contratos”³⁶³.

Si bien es cierto que los Smart Contracts pueden eliminar la ambigüedad y, aunque en principio esto parece un desarrollo positivo, en el derecho contractual la ambigüedad no es un error, sino una característica³⁶⁴ que se deriva de la complejidad del mundo que nos rodea³⁶⁵. Los términos vagos a menudo pueden ser muy eficientes³⁶⁶, en la mayoría

³⁵⁸ Véase RASKIN, M. (2017). "The Law and Legality...", *cit.*, p. 326., DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 72.

³⁵⁹ DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under Contract Law", *cit.* p. 76.

³⁶⁰ PAECH, P. (2016). "The Governance of Blockchain Financial Networks", *LSE Law, Society and Economy*, documento de trabajo No. 16. p. 13. Disponible en: <https://ssrn.com/abstract=2875487> (fecha de consulta: 9 de agosto de 2020).

³⁶¹ RASKIN, M. (2017). "The Law and Legality...", *cit.*, p. 325

³⁶² SCHUSTER, E. (2019). "Cloud Crypto Land", *LSE Law, Society and Economy*, documento de trabajo No. 17, p. 23. Disponible en: <https://ssrn.com/abstract=3476678> (fecha de consulta: 17 de junio de 2020).

³⁶³ GRIGG, I. (2017). "Towards A Ricardian Constitution", *cit.*

³⁶⁴ MIK, E. (2017). "Smart contracts: Terminology...", *cit.*, p. 19.

³⁶⁵ SCHUSTER, E. (2019). "Cloud Crypto Land", *cit.*, p. 23.

³⁶⁶ TRIANTIS, G. (2002). "The Efficiency of Vague Contract Terms: A Response to The Schwartz-Scott Theory of U.C.C. Article 2", *Louisiana Law Review*, vol. 62, p. 1078. Disponible en: <https://digitalcommons.law.lsu.edu/lalrev/vol62/iss4/4> (fecha de consulta: 2 de octubre de 2019).

de los casos, por no decir en todos, es una condición deseable y necesaria. Los contratantes incluyen intencionalmente conceptos indeterminados en sus acuerdos porque de no ser así, las partes tendrían que detallar y prever todas y cada una de las circunstancias futuras que puedan impactar las obligaciones durante la vigencia del negocio jurídico³⁶⁷.

Es probable que los contratantes no puedan llevar a buen término esta empresa, ya que la previsión perfecta, no solo es casi que imposible, sino sumamente costosa³⁶⁸. Por esta razón, en la práctica las partes redactan los contratos de forma incompleta³⁶⁹ porque, al fin y al cabo, como señala PONCIBÒ, el código no es diferente al uso de palabras, pues ambos son creaciones humanas³⁷⁰.

Teniendo en cuenta que para los contratantes puede ser inviable y prohibitivamente alto redactar acuerdos completos, el sistema legal proporciona soluciones a este problema³⁷¹ (Por ejemplo, las costumbres comerciales, los principios generales del derecho)³⁷². Desde luego, hay quienes argumentan que los contratos inteligentes no necesitan del sistema legal para existir, ni de los remedios del mismo, puesto que ellos son una alternativa tecnológica a todo el sistema³⁷³. No obstante, las partes pueden no estar satisfechas, no solo porque existan discrepancias entre ambas, sino también porque los resultados obtenidos no son los esperados, así que mutuo

³⁶⁷ PAECH, P. (2016). "The Governance of Blockchain Financial Networks", *cit.*, p. 29.

³⁶⁸ POSNER, R. (2004). "The Law and Economics of Contract Interpretation", *Texas law Review*, vol 83, p. 1582. Disponible en: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2893&context=journal_articles (fecha de consulta: 19 de septiembre de 2019).

³⁶⁹ HART, O. & MOORE, J. (1988). "Incomplete contracts and renegotiation", *Econometrica: Journal of the Econometric Society*, Vol. 56, No. 4, p. 755. Disponible en: <https://www.jstor.org/stable/1912698> (fecha de consulta: 19 de septiembre de 2019).

³⁷⁰ PONCIBÒ, C. & DIMATTEO, L. (2019). "Smart Contracts Contractual ...", *cit.*, p. 119.

³⁷¹ DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C. (2019). "Smart Contracts and Contract Law", *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, p. 11.

³⁷² En este sentido, GOVERNATORI, G., IDELBERGER, F., MILOSEVIC, Z., RIVERET, R., SARTOR, G. & XU, X. (2018). "On legal contracts... ", *cit.*, p. 382, lo denominan integración contractual, en el cual el contrato se integra con la ley, para abordar los elementos que no fueron previstos por las partes en el momento de la celebración, es decir, si no se indicó algún elemento la ley puede establecer términos por defecto o puede proporcionarles a los jueces criterios para llenar el vacío, véase

³⁷³ SAVELYEV, A. (2017). "Contract law 2.0: Smart contracts as the beginning of the end of classic contract law", *Information & Communications Technology Law*, Vol. 26, No. 2, p. 21. Disponible en: <https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1301036?journalCode=cict20> (fecha de consulta: 29 de febrero de 2019).

consentimiento, una renegociación de los términos contractuales constituye una necesidad y un beneficio deseable.

La ambigüedad no solo les ofrece a las partes flexibilidad para adaptarse a circunstancias sobrevenidas que pueden surgir por cambios regulatorios o comerciales³⁷⁴, sino que también reduce el tiempo y los gastos de negociación³⁷⁵. En este sentido, la naturaleza inherentemente rígida de los contratos inteligentes no supone una característica deseable, sino más bien una limitación, dado que en situaciones cambiantes o imprevistas no tendrán la capacidad de adaptarse a nuevos escenarios. Para que ello ocurra, se deben describir antes que tenga lugar la ejecución del contrato, de forma precisa y completa las posibles circunstancias posteriores que, si bien pueden acercarse, nunca se logrará la perfección³⁷⁶, porque el futuro es inherentemente impredecible³⁷⁷.

Por supuesto, hay quienes podrían argumentar que los Smart Contracts pueden ser susceptibles de modificaciones, sin embargo, como oportunamente sostiene SKLAROFF “tales modificaciones solo pueden hacerse si las partes contemplan explícitamente desde el principio que podrían querer hacer esos cambios particulares más adelante”³⁷⁸; y esto solo es posible, si las mismas gastaron los recursos suficientes para predecir contingencias futuras. En resumen, uno de los supuestos beneficios de los Smart Contracts aumentaría los costos de transacción, así que probablemente el precio de formar acuerdos completos no solo es una quimera, sino que superaría los supuestos beneficios³⁷⁹ que ofrece esta nueva tecnología.

Asimismo, la inflexibilidad puede aislar al contrato del contexto social donde se desarrolla³⁸⁰, desde luego, esto no es bueno porque muchas relaciones comerciales dependen del uso y las costumbres sociales. Nuevamente, algunos podrían alegar que los contratos inteligentes que se ejecutan en una Blockchain no necesitan de un contexto

³⁷⁴ MIK, E. (2017). “Smart contracts: Terminology...”, *cit.*, p. 22.

³⁷⁵ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 77.

³⁷⁶ PAECH, P. (2016). “The Governance of Blockchain Financial Networks”, *cit.*, p. 29.

³⁷⁷ POSNER, R. (2004). “The Law and Economics of...”, *cit.*, p. 1582.

³⁷⁸ SKLAROFF, J. (2017). “Smart Contracts and the ...”, *cit.*, pp. 280. 291.

³⁷⁹ DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C. (2019). “Smart Contracts and Contract Law”, *cit.*, p. 11.

³⁸⁰ Señala LEVY, K. (2017). “Book-Smart, Not Street-Smart...”, *cit.*, que los contratos cumplen funciones que no son estrictamente legales y que muchas veces los contratos se hacen cumplir con mecanismos sociales. Véase también MIK, E. (2017). “Smart contracts: Terminology...”, *cit.*, p. 20.

social preexistente, ni mucho menos de una autoridad central o intermediario institucionalizado, ya que esta tecnología ofrece un nuevo y mejorado mecanismo de confianza para el comercio, pues las partes ya no necesitan de un sistema legal que garantice el cumplimiento de sus obligaciones (que muchas veces puede ser deficiente o nulo) sino que dicha tecnología proporciona tal confianza³⁸¹.

Sin embargo, si hay una consecuencia indeseable, los contratantes no tienen más posibilidades que las previamente descritas en el código y, allí es cuando la función social de los sistemas de contratación tradicionales facilita la entrada de costumbres y usos comerciales, hecho que permite que se adapten a la complejidad del mundo real.

La rigidez de los contratos inteligentes también amenaza su adopción en masa, porque tal y como señala MIK³⁸², desde una perspectiva comercial no es atractivo que un contrato se ejecute independientemente de las circunstancias adyacentes. En definitiva, el derecho contractual es dinámico, indudablemente ello puede acarrear diversas interpretaciones que pueden dar lugar a disputas, pero la flexibilidad también es la génesis de la innovación³⁸³.

2. Contratos inteligentes y semántica legal

2.1 Límites del lenguaje

El proceso de traducción de un contrato legal a un código de contrato inteligente crea problemas al derecho contractual, pues la forma en que funciona el lenguaje natural es distinta a la forma de cómo opera el lenguaje formal, lo que inevitablemente genera ciertos límites a la hora de transponer el acuerdo al código, porque a pesar de que ambos lenguajes consisten en un contenido simbólico estructurado tienen características que difieren³⁸⁴.

³⁸¹ EENMAA-DIMITRIEVA, H. & SCHMIDT-KESSEN, M.J. (2019). "Creating markets ...", *cit.*, p. 70.

³⁸² MIK, E. (2019). "Smart Contracts...", *cit.*, p. 21.

³⁸³ DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C. (2019), *Op. Cit.*, p. 9.

³⁸⁴ ALLEN, J. (2018). "Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Languages", *European Review of Contract Law*, Vol.14, No. 4, p. 323. Disponible en: <https://doi.org/10.1515/ercl-2018-1023> (fecha de consulta: 12 de junio de 2020).

2.2 Estudio del lenguaje

Señala el historiador YUVAL NOAH HARARI que “Homo sapiens conquistó el mundo gracias, por encima de todo, a su lenguaje único”³⁸⁵, pues la flexibilidad del lenguaje permitió que pudiésemos comunicarnos, transmitir una cantidad ingente de información no solo del mundo que nos rodeaba, sino también sobre ficciones.

Nuestro lenguaje siempre ha estado en constante evolución e incluso hemos sido capaces de desarrollar nuevas formas de comunicarnos, por ejemplo, hemos inventado lenguajes lógicos que son capaces de transmitir órdenes e información que pueden ser comprendidos por las máquinas.

La multiplicidad de signos abrió una alta gama de posibilidades de significados distintos, que actualmente son estudiados por la semiótica, ciencia que se encarga de su análisis mediante tres grandes disciplinas, a saber, la sintaxis, la semántica y la pragmática.

i. Sintaxis

La sintaxis estudia las relaciones entre signos, es decir, analiza “el modo en que se combinan las palabras y los grupos que estas forman para expresar significados, así como las relaciones que se establecen entre todas esas unidades”³⁸⁶. En otras palabras, nos permite darle un sentido coherente a la forma en cómo nos comunicamos.

ii. Semántica

La semántica es el estudio del significado de los signos, es decir, la relación entre las palabras y su significado e interpretación. Advierte ALLEN que “el contenido semántico de un lenguaje natural es difícil de formalizar y hacer legible por máquina. Hay más matices de significado y ambigüedad en el lenguaje natural de lo que sería posible en un lenguaje formal”³⁸⁷. Por ejemplo, una oración escrita en lenguaje natural puede tener distintos significados, aunque su sintaxis sea la misma, hecho que no sucede con los

³⁸⁵ HARARI, Y. N. (2014). *Sapiens. De animales a dioses: una breve historia de la humanidad*. Debate, pp. 26-27.

³⁸⁶ “Sintaxis”. (Sin fecha). Disponible en: <https://dle.rae.es/sintaxis> (fecha de consulta: 12 de enero de 2021).

³⁸⁷ ALLEN, J. (2018). “Wrapped and Stacked...”, *cit.*, p. 323.

lenguajes formales, ya que la semántica de estos es más estricta y matemáticamente precisa.

iii. Pragmática

La pragmática estudia la relación entre las palabras y el contexto en el que se pronuncian, es decir, una misma oración puede tener distintos significados dependiendo del contexto en la cual se manifiestan. Como hemos mencionado anteriormente, las máquinas no son buenas para inferir el contexto en el que se enuncian las palabras y, por tanto, tampoco son tan adecuadas como los humanos para esta disciplina, es más, hay que tener en cuenta que es poco probable que un programador comprenda el contexto en el cual se desenvuelve un contrato legal, pues este se desarrolla de acuerdo a una ontología jurídica, es decir, un conjunto de conceptos y categorías jurídicas, con sus definiciones y propiedades³⁸⁸.

3. Relación de los lenguajes

Los lenguajes de programación son más limitados y estrictos que los lenguajes naturales, así que, a la hora de programar un acuerdo legal (con todos los significados que puede contener un signo), a un código de contrato inteligente, el cual está estructurado en una lógica binaria, consecuentemente habrá obstáculos y límites a la hora de intentar representar la diversidad y complejidad del derecho contractual.

Por ejemplo, suponga una cláusula de pago que ha sido transpuesta al código (y no tiene un respaldo en papel) si una de las partes no está satisfecha con los resultados obtenidos porque la cláusula codificada no representa lo acordado, ello puede acarrear dificultades probatorias en cuanto a lo estipulado³⁸⁹.

El código de contrato inteligente siempre va a estar relacionado con el lenguaje natural, porque, aunque se codifique directamente, es muy probable que las partes lo

³⁸⁸ CLACK, C. (2018). "Smart Contract Templates: legal semantics and code validation", *Journal of Digital Banking*, Vol. 2, no 4, p. 4. Disponible en: https://www.researchgate.net/publication/335465751_Smart_Contract_Templates_legal_semantics_and_code_validation C. D. Clack *Journal of Digital Banking* 24 338-352 2018 (fecha de consulta: 16 de julio de 2020).

³⁸⁹ Ejemplo descrito por MIK, E. (2019). "Smart Contracts...", *cit.*, p. 20.

hayan concebido en sus mentes y acordado en lenguaje humano. De tal manera que la traducción o transposición del lenguaje natural a uno que el ordenador pueda comprender, debe ser isomorfo, para que las partes puedan estar completamente seguras, que el código refleja fielmente sus intenciones. Aunque, como advierte ALLEN, esto no es posible y puede que nunca lo sea por la divergencia de funcionamiento de ambos lenguajes.³⁹⁰ No obstante, existen esfuerzos desde la doctrina por intentar que la transposición sea lo más equivalente.

Siendo así, cómo pueden estar los contratantes seguros que el código es una representación equivalente de lo que se acordó en lenguaje natural. Antes de abordar las propuestas ideadas desde la academia, debemos abordar la semántica de un contrato legal, para saber la composición de su estructura.

i.Semántica de los contratos legales inteligentes

Advierte, con acierto, VON WENDLAND que el término semántica “hace referencia al proceso de creación de protocolos digitales para obtener certeza del significado de un lenguaje de programación”³⁹¹, es decir, es la manera de cómo podemos estar seguros del significado del código de contrato inteligente.

Para conocer la semántica de un acuerdo legal es necesario mencionar que las cláusulas de un contrato se han dividido en dos, las operacionales y las no operacionales³⁹². Algunas cláusulas son automatizables y otras no.

ii.Cláusulas operacionales

Las cláusulas operacionales hacen referencia a las partes operativas del contrato, esto es, son las cláusulas que son susceptibles de automatización, por lo que están

³⁹⁰ ALLEN, J. (2018). “Wrapped and Stacked...”, *cit.*, p. 336.

³⁹¹ VON WENDLAND, M. (2018). “Smart contracts that are smart and can function as legal contracts - A Review of Semantic Blockchain and Distributed Ledger Technologies”. Disponible en: <https://arxiv.org/abs/1805.01279> (fecha de consulta: 7 de diciembre de 2020).

³⁹² ISDA & LINKLATERS. (2017). “Whitepaper Smart Contracts ...”, *cit.*, p. 10. También utilizan esta misma distinción, CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). “Smart Contract Templates: foundation ...”, *cit.*, pp. 1 y ss.

relacionadas con la ejecución del contrato³⁹³. Señala un documento blanco de ISDA, que por lo general estas cláusulas incluyen alguna forma de lógica condicional, es decir, que para que ocurra un hecho, es necesario la ocurrencia de una acción determinista³⁹⁴. Un ejemplo de este tipo de cláusula es una que haga referencia al pago.

iii. Cláusulas no operacionales

Las cláusulas no operaciones son aquellas partes del acuerdo que no deseamos automatizar o que no son automatizables³⁹⁵. Dicho de otra forma, son disposiciones que no incorporan la lógica condicional propia de los aspectos operacionales. Un ejemplo de este tipo de cláusula es una de sumisión a fuero en un préstamo hipotecario, o una cláusula que establezca la ley aplicable al contrato que estipule que una de las partes debe actuar con buena fe, o realizar verificaciones de diligencia debida.

3.1 ¿Cómo podemos superar estas limitaciones?

Son varias las propuestas que se han sugerido desde la academia para que los contratantes estén seguros de que existe una correspondencia de los derechos y obligaciones que han acordado, con lo representado en el código. Algunas propuestas han sugerido la validación del código, otras, en cambio, han apuntado a que repensemos la forma en cómo redactamos los contratos, es decir, apuntan a que escribamos contratos más formales. Veamos de qué se tratan cada una.

3.1.1 Validación del código de contrato inteligente

Hay quienes como CLACK³⁹⁶ proponen la validación del código del contrato inteligente de los acuerdos de derivados financieros, los cuales son altamente regulados,

³⁹³ CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). "Smart Contract Templates: foundations...", *cit.*, p. 5

³⁹⁴ ISDA & LINKLATERS. (2017). "Whitepaper Smart Contracts ...", *cit.*, p. 10.

³⁹⁵ CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). "Smart Contract Templates: foundations...", *cit.*, p. 5.

³⁹⁶ CLACK, C. (2018). "Smart Contract Templates...", *cit.*, p. 1.

extensos y complejos³⁹⁷. La validación se realiza con el objetivo de verificar si el código desempeñará correctamente las disposiciones del contrato legal.

Dicho autor hace una distinción entre probar y validar, pues probar es asegurarse de que el contrato no contenga errores y validar es verificar que el código sea fiel al significado del contrato, es decir, a su semántica legal. Esta es la parte más difícil, pues requiere que el desarrollador comprenda la documentación legal³⁹⁸. Advierte que validar no se trata de ejecutar el código para verificar que no se produzcan errores, tampoco es una cuestión de comprobar que los valores de salida sean correctos de acuerdo a varias fórmulas matemáticas o lógica operativa, sino más bien, es una comprensión de la semántica del contrato para proporcionar un conjunto de escenarios de validación. La validación también serviría para que el código se detenga cuando surja una circunstancia inesperada³⁹⁹.

La validación se realiza mediante un análisis semántico formal del texto legal, que proporciona una base firme para generar un conjunto de escenarios de validación, mejorando así la calidad de validación del código. Son muchos los beneficios que, según el autor, brinda este análisis, dentro de los cuales incluye que, puede ayudar a los abogados a aclarar cláusulas oscuras y a exponer los errores en el código. Lógicamente, la validación no es una tarea fácil, pues existe una “brecha pragmática” entre abogados y desarrolladores, por tanto, el jurista debe saber de programación y el programador debe conocer de derecho⁴⁰⁰.

3.1.2 Creación de un lenguaje equivalente

Se debe cerrar la brecha entre la semántica del abogado y la semántica operacional, porque si no ello puede provocar riesgos⁴⁰¹, por este motivo, sugieren la

³⁹⁷ CLACK propone la codificación de las plantillas estandarizadas de los contratos financieros diseñadas por ISDA, que en España se conocen como Contrato Marco de Operaciones Financieras, mediante el contrato Ricardiano propuesto por IAN GRIGG.

³⁹⁸ CLACK, C. (2018). “Smart Contract Templates...”, *cit.*, p. 7.

³⁹⁹ En este sentido CLACK, C. (2018). “Smart Contract Templates...”, *cit.* 7-8, representa estos escenarios de validación, como por ejemplo que sucede si una de las partes realiza el pago parcial.

⁴⁰⁰ CLACK, C. (2018). “Smart Contract Templates...”, *cit.* pp. 14 y ss.

⁴⁰¹ Al respecto AL KHALIL, F., CECI, M., O'BRIEN, L. & BUTLER, T. (2017). “A Solution for the Problems ...”, *cit.*, p. 3, no clasifican la semántica del contrato entre cláusulas operaciones y no operacionales, sino que en cambio lo clasifican entre semántica denotacional, su semántica legal, comercial y regulatoria.

creación de un lenguaje de contratos que sea legible por humanos y por máquinas, para resolver el problema de la traducción, de tal manera que así se garantiza la certeza de que la semántica legal está representada en el código.

Los autores advierten que la confianza en esta tecnología depende de la capacidad de los abogados para comprender, expresar y validar la semántica denotacional de un contrato, sin embargo, indican que actualmente un abogado no puede comprender el comportamiento del código del contrato inteligente porque no existe un lenguaje intermedio que cierre esa brecha⁴⁰².

Proponen que el contrato inteligente debe ser creado por un abogado y por un desarrollador, pero la comunicación entre estos debe estar regida por un lenguaje común y controlado por ambos, al que han denominado como *legal natural language* (en español, lenguaje jurídico natural) en el cual el jurista redacta el acuerdo en un lenguaje lógico, claro, inequívoco y comprensible para el programador⁴⁰³.

4. Consideraciones finales del lenguaje

Hemos mencionado a lo largo de este capítulo que es muy probable que las versiones exitosas que veremos de contratos inteligentes tengan un acuerdo en papel de respaldo, no solo por seguridad jurídica, sino también porque hay elementos o partes del contrato que no son susceptibles para su representación en el código, (o también puede que las partes deseen que haya subconjuntos del contrato que permanezcan fuera de Blockchain). Por tanto, los Smart Contracts son más bien un mecanismo o una herramienta de apoyo para garantizar la ejecución de segmentos automatizables.

Consideramos que a pesar de todos los esfuerzos de la academia por intentar superar los desafíos que supone la representación de conceptos legales (ambiguos, complejos, vagos) a un código de lógica condicional, es improbable que se pueda programar toda la documentación legal al código de contrato inteligente, pues a pesar de los avances que han habido en el desarrollo del *Internet Of Things* (internet de las cosas),

⁴⁰² AL KHALIL, F., CECI, M., O'BRIEN, L. & BUTLER, T. (2017). "A Solution for the Problems ...", *cit.*, p. 8.

⁴⁰³ AL KHALIL, F., CECI, M., O'BRIEN, L. & BUTLER, T. (2017). "A Solution for the Problems ...", *cit.*, pp. 10-11.

los contratos inteligentes no pueden controlar objetos del mundo físico, no pueden ejecutar la entrega de un bien o la prestación de un servicio. En fin, no se puede codificar el comportamiento humano. En realidad, ¿a quién y cómo beneficia esta rigidez? No tiene sentido que codificar la obligación de que un contratante actúe de buena fe o haga verificaciones de diligencia debida. Así que, es improductivo intentar trasponer al código cláusulas ambiguas que las máquinas no podrán ejecutar ⁴⁰⁴. Este desafío es y seguirá siendo un problema del mundo analógico.

⁴⁰⁴ MIK, E. (2019). “Smart Contracts...”, *cit.*, p. 20.

CAPÍTULO TRES

LA PROTECCIÓN DE LOS CONSUMIDORES DE CRIPTOACTIVOS: RETOS REGULATORIOS

CAPÍTULO TRES: LA PROTECCIÓN DE LOS CONSUMIDORES DE CRIPTOACTIVOS: RETOS REGULATORIOS

I. LA PROTECCIÓN DE LOS CONSUMIDORES DE CRIPTOACTIVOS: RETOS REGULATORIOS

1. Introducción

Los últimos avances tecnológicos, en especial los cambios que se están introduciendo con la tecnología Blockchain, está creando nuevos activos financieros y nuevos modos de intermediación⁴⁰⁵. Nuestra comprensión del dinero y la propiedad cambia a medida que el consumo se vuelve digital⁴⁰⁶. Se cree la tecnología Blockchain tiene la capacidad de empoderar a los consumidores. Entre los beneficios que, según la doctrina, representa esta tecnología para los consumidores encontramos, el envío y recepción de dinero de forma instantánea, bajas tarifas, acceso a mercados financiero de grupos históricamente excluidos⁴⁰⁷, microcréditos, comercio electrónico descentralizado⁴⁰⁸, autenticidad⁴⁰⁹, préstamos entre consumidores, y lo más importante, la desaparición del supuesto “peor intermediario”, el banco. Sin embargo, como señala el Departamento del Tesoro de los EEUU en un informe publicado en 2022⁴¹⁰, los datos disponibles actualmente indican que la realización de tales beneficios ha sido limitada. Por ejemplo, los costos de transacción no son bajos, en las cadenas de bloques públicas

⁴⁰⁵ ESMA. (2022). *TRV Risk Analysis Crypto-assets and their risks for financial stability*, Luxembourg, p.3. Disponible en: https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf (fecha de consulta: 18 de octubre de 2022).

⁴⁰⁶ BELK, R., HUMAYUN, M., & BROUARD, M. (2022). “Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets”, *Journal of Business Research*, Vol. 153, pp.198-205. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0148296322007147> (fecha de consulta: 23 de septiembre de 2022).

⁴⁰⁷ FOSTER-FRAU, S. (2021) “Locked out of traditional financial industry, more people of color are turning to cryptocurrency”. Disponible en: https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa-37fe-11ec-9bc4-86107e7b0ab1_story.html (fecha de consulta: 15 de agosto de 2022).

⁴⁰⁸ QUIROZ-RUIZ, A. (2020). “Cuestiones jurídicas del comercio electrónico en Blockchain”, *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (Dirs. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra. pp. 871-903.

⁴⁰⁹ SCHLEGEL, M., ZAVOLOKINA, L., & SCHWABE, G. (2018). “Blockchain technologies from the consumers’ perspective: What is there and why should who care?”. *Proceedings of the 51st Hawaii international conference on system sciences*, pp. 3480-3482 Disponible en: <https://www.blockchain.uzh.ch/wp-content/uploads/paper0442-1.pdf> (fecha de consulta: 10 de septiembre de 2022).

⁴¹⁰ U.S. DEPARTMENT OF THE TREASURY (2022). *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, p.41. Disponible en: https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf (fecha de consulta: 3 de octubre de 2022).

de prueba de trabajo o prueba de participación, los mineros son quienes seleccionan y organizan qué transacciones incluir dentro de los bloques que están introduciendo, por lo que tendrán preferencia por las que ofrecen tarifas más altas, dejando inviables las microtransacciones. El costo promedio de una transacción en bitcoin, en momentos de mayor actividad, ronda los 150 dólares⁴¹¹. Asimismo, la caída de los precios de las criptomonedas en aproximadamente el 65% de su valor a lo largo del 2022, ha supuesto pérdidas más graves para los inversionistas pertenecientes a grupos vulnerables, pues estos tienen menos posibilidades de contar con recursos financieros para absorber las pérdidas⁴¹².

En 2008, Satoshi Nakamoto presentaba Bitcoin al mundo como una alternativa al sistema financiero tradicional, una moneda descentralizada que no dependiera de ningún intermediario o autoridad central que ejerciera control. A partir de ese momento, surgieron un sinnúmero de variedades de criptomonedas y proyectos criptográficos que se aprovecharon de la elusión regulatoria⁴¹³. El sector donde más creció dicha tecnología, fue precisamente del lugar de donde surgió, las finanzas. En este ecosistema las finanzas son descentralizadas (DeFi, abreviatura de *Decentralized Finance*), un mercado financiero sin intermediarios que utiliza la tecnología Blockchain como base. Ha tenido un impulso en los últimos años gracias al desarrollo de la web 3.0. No obstante, el desarrollo de DeFi ha dejado al descubierto un problema mundial que se exacerbó con la pandemia de la COVID-19 del año 2020, el mercado de criptoactivos está plagado de estafas, robos y negligencias técnicas y operativas.

A pesar de los riesgos que implican los criptoactivos, los consumidores empezaron a invertir principalmente con su cartera de ahorros. Los pequeños inversionistas representan un número importante del total de los inversores de criptoactivos, según la encuesta de expectativas de los consumidores del Banco Central

⁴¹¹ ROSENTHAL, D. (2022). "Regulating "Digital Assets". Disponible en: <https://blog.dshr.org/2022/07/regulating-digital-assets.html> (fecha de consulta: 1 de septiembre de 2022).

⁴¹² CACHERO, P. (2022). "Crypto Collapse Threatens to Leave Black, Hispanic Investors Further". Disponible en: <https://www.bloomberg.com/news/articles/2022-07-07/crypto-collapse-threatens-to-leave-black-hispanic-investors-further-behind> (fecha de consulta: 23 de septiembre de 2022).

⁴¹³ QUAMARA, S., & SINGH, A. K. (2022). "A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives". *Computers & Security*, Vol. 113. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404821003722> (fecha de consulta: 10 de septiembre de 2022).

Europeo⁴¹⁴ el 10% de los hogares de la Unión Europea posee criptoactivos. Es decir, el mercado ha aumentado y se ha desarrollado sin un marco regulatorio definido.

No obstante, la ausencia de intermediarios y/o de una autoridad central no implica más protección, sino todo lo contrario, indefensión, pues como hemos mencionado existen muchos riesgos asociados y la protección a los consumidores no está garantizada, ya que la aplicación de las leyes de protección al consumidor vigentes de la Unión Europea⁴¹⁵ son limitadas. En contraste de lo que sucede en el sistema financiero tradicional, cuyos actores y productos están sometidos a estrictos controles, que sirven como mecanismos de protección para los consumidores. En este sentido, el considerando 3 la propuesta de Reglamento relativo a los mercados de criptoactivos aclara que debido a que la mayoría de los criptoactivos quedan por fuera de la legislación europea en relación con los servicios financieros (MIFID II), no existe una normatividad aplicable “para los servicios relacionados con los criptoactivos, ni siquiera en lo tocante a la explotación de plataformas de negociación de criptoactivos, el canje de criptoactivos por moneda Fiat u otros criptoactivos, o la custodia de criptoactivos”⁴¹⁶. Esta falta de regulación deja a los consumidores desprotegidos frente a los riesgos asociados con la adquisición y tenencia de estos activos.

La mayoría de los criptoactivos, como Bitcoin, no tiene un valor en el mundo real, al contrario que las acciones que cotizan en la bolsa de valores que, les otorgan a sus titulares una participación fraccionada del capital de una empresa. De ahí que, la mayor parte de estos activos sean especulativos y, por tanto, volátiles, lo que implica que su valor dependa exclusivamente de las dinámicas de la oferta y demanda⁴¹⁷. Aunque si tenemos en cuenta el seudonimato de la red, es difícil determinar si los precios y los volúmenes de las transacciones son reales o son el resultado de una negociación manipulada, del empleo de bots para operar varias carteras, o de un grupo de personas

⁴¹⁴ La encuesta se llevó a cabo en 2021 en 6 países de la eurozona: Bélgica, Alemania, España, Francia, Italia y Holanda, véase HERMANS, L., IANIRO, A., KOCHANASKA, U., TÖRMÄLEHTO, V. M., VAN DER KRAAIJ, A., & SIMÓN, J. M. V. (2022), “Decrypting financial stability risks in crypto-asset markets. *Financial Stability Review*”, No. 1. Disponible en: https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html (fecha de consulta: 12 de septiembre de 2022).

⁴¹⁵ NEWS EUROPEAN PARLIAMENT. (2022). “Cryptocurrency dangers and the benefits of EU legislation”. Disponible en: <https://www.europarl.europa.eu/news/en/headlines/economy/20220324STO26154/cryptocurrency-dangers-and-the-benefits-of-eu-legislation> (fecha de consulta: 13 de octubre de 2022).

⁴¹⁶ Considerando 3 de la propuesta.

⁴¹⁷ ESMA. (2022). *TRV Risk Analysis...*, Op. Cit., p. 12.

que actúan de forma colusoria⁴¹⁸. Las criptomonedas han venido siendo empleadas como productos de inversión y en menor medida como medio de pago.

Los riesgos del mercado de los criptoactivos no solo se dan por la alta volatilidad, la falta de transparencia, y asimetría de la información, sino también por los fraudes, robos y estafas. Tal como lo advierte la Autoridad Europea de Valores y Mercados ESMA (por sus siglas en inglés, *European Securities and Markets Authority*), el problema se agrava con las campañas agresivas de marketing a través de redes sociales y de influencers⁴¹⁹, así como por el respaldo público e impulso de celebridades de la talla de Kim Kardashian, Neymar o Elon Musk, o porque las fuentes de asesoría sobre inversiones sean las comunidades de TikTok o YouTube.

El presente capítulo tiene por objetivo esbozar los principales riesgos que representa para los consumidores y usuarios operar con criptoactivos, así como analizar las medidas tomadas por la unión europea para salvaguardar a los usuarios en la propuesta de Reglamento sobre criptoactivos. Para hacerlo, primero definiremos algunos conceptos claves del ecosistema cripto. Luego, en segundo lugar, analizaremos los riesgos de los criptoactivos y los problemas de la centralización de la tecnología Blockchain. A continuación, en tercer lugar, destacaremos las advertencias emitidas por las autoridades financieras europeas para alertar sobre criptoactivos, en especial las criptomonedas. Finalmente, y, en cuarto lugar, examinamos las medidas introducidas en la propuesta de Reglamento para proteger a los consumidores. Concluimos que, si bien la propuesta de legislación no protege a los consumidores en todos los riesgos, es una reglamentación necesaria y bienvenida, dada las fallas y asimetrías detectadas en la presente sección.

i. *Criptoactivos*⁴²⁰. Los criptoactivos son una representación digital de valores y derechos que pueden transferirse o almacenarse electrónicamente usando la tecnología del libro mayor distribuido (DLT).⁴²¹ Los criptoactivos pueden adoptar muchas formas y

⁴¹⁸ U.S. DEPARTMENT OF THE TREASURY (2022). *Crypto-Asset...*, *Op. Cit.*, p. 32

⁴¹⁹ ESMA. (2022). *TRV Risk Analysis...*, *Op. Cit.*, p. 5.

⁴²⁰ A lo largo de este trabajo cuando hablemos de criptoactivo no estaremos refiriendo de forma genérica a todas las representaciones digitales de valores y derechos que puedan adoptar.

⁴²¹ BANCO DE ESPAÑA (2022). *Informe de estabilidad financiera. Primavera 2022*, p.152. Disponible en: https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinanciera/22/IEF_Primavera2022.pdf (fecha de consulta: 11 de septiembre de 2022).

características como criptomonedas, quizás el criptoactivo más popular; fichas (token, como los *utility token* o Ficha de servicio), NFT (*tokens no fungibles*), *stablecoin*, etc.

ii. *Non-fungible tokens* o NFT. Los NFT son “objetos digitales que contienen referencias a otros activos, físicos o digitales”⁴²², en otras palabras, son tokens criptográficos que se pueden emplear para representar la propiedad de activos únicos⁴²³ como una obra de arte, una canción, un videojuego, unas escrituras etc. Aunque los NFT se pueden comprar y vender en un mercado de NFT, no son intercambiables, esto significa que cada token es único o no fungible, a diferencia de las criptomonedas que son fungibles lo que quiere decir que pueden intercambiarse entre sí.

Los NFT se registran en una Blockchain, generalmente se emplea Ethereum, aunque pueden existir en otras cadenas de bloques⁴²⁴, y se crean y gestionan mediante un Smart Contracts. Habida cuenta que en una Blockchain el almacenamiento suele ser limitado, lo que se guarda en esta no es el activo en sí mismo, (aunque si no es muy pesado puede que sí), sino “su huella digital (o el llamado *hash*); y lo que es más importante, metadatos que describen tanto los atributos elegidos del objeto tokenizado, como un puntero al objeto del mundo real que se tokeniza”⁴²⁵, es decir, que en la Blockchain lo que se almacena es una dirección web o un hash que apuntan al sitio donde se encuentra realmente almacenado.

iii. *Billetera o monedero (Wallets)*. Es una dirección, determinada por su clave pública, que puede enviar y recibir criptoactivos. La clave privada se usa para firmar las transacciones y debe ser mantenida en secreto por el propietario⁴²⁶. Los monederos se

⁴²² KOOLEN, C. (2022). “Apes Gone’, but What about Consumer Protection? Applying EU Consumer Law to the Transfer of NFTs. Applying EU Consumer Law to the Transfer of NFTs”. Disponible en: <https://law.kuleuven.be/ccm/blog/?p=289> (fecha de consulta: 17 de septiembre de 2022).

⁴²³ “Non-fungible tokens (NFT)”. (Sin fecha). Disponible en: <https://ethereum.org/en/nft/> (fecha de consulta: 12 de septiembre de 2022).

⁴²⁴ CONTI, R. & SCHMIDT, J. (2022). “What Is An NFT? Non-Fungible Tokens Explained”. Disponible en: <https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/> (fecha de consulta: 12 de septiembre de 2022).

⁴²⁵ BODÓ, B., GIANNOPOULOU, A., QUINTAIS, J., & MEZEI, P. (2022). “The rise of NFTs: These aren't the droids you're looking for”, p. 6. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4000423 (fecha de consulta: 12 de septiembre de 2022).

⁴²⁶ INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS. (2020). *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms*. Disponible en: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf> (fecha de consulta: 23 de abril de 2021).

usan para el almacenamiento de claves⁴²⁷ (pública y privada), pues a diferencia de un monedero del mundo físico, en el cual el usuario puede guardar dinero en efectivo, en los monederos de criptoactivos, no se almacena criptoactivos, ya que estos se alojan en la cadena de bloques y solo se puede acceder a ellos mediante la clave privada⁴²⁸, que es la que tiene el control de los fondos que posea ese usuario⁴²⁹.

Los usuarios suelen emplear monederos criptográficos que pueden ser fríos o calientes. Un monedero caliente es una billetera criptográfica que está conectada a internet que, puede ser de escritorio, es decir, un programa instalado en el ordenador como Exodus o Electrum. También puede ser móvil, esto es, una aplicación para el smartphone, como Bitpay o Binance, o puede que sea web, que son los monederos alojados por las casas de cambio, como Coinbase o Binance. Mientras que, un monedero frío no está conectado a internet y puede ser un *hardware*, como un pendrive o una tarjeta inteligente, o estar escrito en un pedazo de papel⁴³⁰. Los monederos fríos suelen ser los más seguros, pues al no estar conectados a la red es difícil que sufran ataques piratas y, es el usuario quien ejerce el control de sus fondos, ya que, en muchas billeteras calientes, las claves suelen estar controladas por terceros. No obstante, en caso de pérdida de la contraseña o destrucción del *hardware*, no hay forma de recuperar la contraseña que controla esos fondos.

Para la custodia de criptoactivos, generalmente los usuarios emplean monederos de custodia, a veces llamados monederos alojados⁴³¹, que funcionan de forma parecida a los bancos, pues permiten el almacenamiento y custodia de los criptoactivos y facilita su compra, venta y transferencia. Sin embargo, el usuario no ejerce control sobre su clave privada, sino que es la plataforma quien la controla en nombre del consumidor.

⁴²⁷ SUNG, S. (2021). "A new key protocol design for cryptocurrency wallet". *ICT Express*, Vol. 7, No. 3. Disponible en: <https://www.sciencedirect.com/science/article/pii/S2405959521000904> (fecha de consulta: 28 de agosto de 2022).

⁴²⁸ "¿Qué es una billetera de criptomonedas?". (Sin fecha). Disponible en: <https://www.coinbase.com/es-LA/learn/crypto-basics/what-is-a-crypto-wallet> (fecha de consulta: 12 de septiembre de 2022).

⁴²⁹ REZAEIGHALEH, H., & ZOU, C. C. (2019). "Deterministic sub-wallet for cryptocurrencies", *2019 IEEE International Conference on Blockchain*. Disponible en: <https://ieeexplore.ieee.org/abstract/document/8946154/references#references> (fecha de consulta: 28 de agosto de 2022).

⁴³⁰ TAYLOR, S. K., ARIFFIN, A., ARIFFIN, K. A. Z., & ABDULLAH, S. (2021). "Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets", In *2021 3rd International Cyber Resilience Conference*. Disponible en <https://ieeexplore.ieee.org/abstract/document/9392446/authors#authors> (fecha de consulta: 28 de agosto de 2022).

⁴³¹ U.S. DEPARTMENT OF THE TREASURY (2022). *Crypto-Asset..., Op. Cit.*, p. 6.

Generalmente, los monederos de custodia son ofrecidos por las plataformas de intercambio de criptoactivos como Coinbase, Binance o Kraken, que crean una experiencia e interfaz de usuario similar a la de los bancos. No obstante, estos servicios están sometidos a las normas de KYC/AML (que puede ser no deseable para los entusiastas del “anonimato”). En caso de pérdida de la contraseña, el usuario la puede recuperar, ya que se accede a ella a través de un usuario y contraseña tradicional y no mediante la clave público privada (criptografía asimétrica).

iv. *Plataformas de intercambios o casas de cambio (Exchange)*. Son plataformas que permiten la compra, venta e intercambio de criptoactivos (criptomonedas, NFT, *stablecoin*, etc.) por otros criptoactivos o dinero Fiat. Según datos de CHAINALYSIS, representa la categoría de servicio más importante y más utilizada en esta industria y suele ser el lugar más común para que los nuevos usuarios adquieran criptomonedas⁴³².

Las plataformas de intercambio pueden ser centralizadas o descentralizadas. Las casas de cambio centralizadas son más populares y más usadas que las descentralizadas⁴³³. Tienen la custodia de los criptoactivos y funcionan como las casas de cambio tradicionales, estableciendo los precios de diversas monedas y cobrando una tarifa por el servicio que prestan⁴³⁴. Estas plataformas ofrecen una variedad de servicios adicionales, como el comercio, el préstamo, el empréstito y generalmente cumplen con los requisitos de KYC/AML⁴³⁵.

Mientras que, las plataformas descentralizadas funcionan de forma parecida a las plataformas centralizadas, pero sin la presencia de intermediarios que controlen los

⁴³² CHAINALYSIS (2021) *Who's Who on the Blockchain? Mapping the Key Players in the Cryptocurrency Ecosystem*, pp. 9-10. Disponible en: <https://go.chainalysis.com/rs/503-FAP-074/images/Key-players-in-crypto-report.pdf> (fecha de consulta: 15 de septiembre de 2022).

⁴³³ ASPRIS, A., FOLEY, S., SVEC, J., & WANG, L. (2021). “Decentralized exchanges: The “wild west” of cryptocurrency trading”, *International Review of Financial Analysis*, Vol. 77. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S1057521921001782#fn0015> (fecha de consulta: 18 de agosto de 2022).

⁴³⁴ COLLIER, K. (2021). “Crypto exchanges keep getting hacked, and there's little anyone can do”. Disponible en: <https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870> (fecha de consulta: 21 de agosto de 2022).

⁴³⁵ INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS. (2022). *IOSCO decentralized finance report*, p. 16. Disponible en: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> (fecha de consulta: 18 de septiembre de 2022).

fondos o los monederos. Estas plataformas se gestionan de forma descentralizada y las transacciones se llevan a cabo entre pares. No están sometidas a las normas KYC/AML.

2. Estafas, pérdidas de dinero y riesgos

A día de hoy los esfuerzos legislativos se han centrado principalmente en abordar los riesgos asociados con el blanqueo de capitales, financiación del terrorismo y la importancia fiscal de las criptomonedas⁴³⁶. A nivel europeo, cabría destacar la Directiva relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo⁴³⁷.

A nivel local, en España las plataformas de intercambio de criptomonedas y las billeteras deben registrarse en el registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos del Banco de España⁴³⁸. La inscripción en este registro está únicamente condicionada a “la existencia de procedimientos y órganos adecuados de prevención de blanqueo de capitales y de financiación del terrorismo, y al cumplimiento de los requisitos de honorabilidad comercial y profesional”. Sin embargo, que una casa de cambio se registre no significa que sea confiable, puesto que tal y como menciona el Banco Central Español, dentro de sus funciones no está la de supervisar los riesgos financieros u operativos y de seguridad, ni tiene ninguna competencia en materia de conducta sobre estos proveedores⁴³⁹.

⁴³⁶ POELMAN, M., & IQBAL, S. (2021). “Investigating the compliance of the GDPR: Processing personal data on a blockchain”, *IEEE 5th International Conference on Cryptography, Security and Privacy*. Disponible en <https://ieeexplore.ieee.org/abstract/document/9357590> (fecha de consulta: 14 de septiembre de 2022).

⁴³⁷ DIRECTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE

⁴³⁸ España. Ley 10/2010 de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado*, 28 de abril de 2010.

⁴³⁹ BANCO DE ESPAÑA (2022). “Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos”. Disponible en: https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html (fecha de consulta: 21 de octubre de 2022).

Sin embargo, la protección al consumidor no se ha tenido mucho en cuenta en las agendas legislativas europeas, ni locales, aunque, como tendremos oportunidad de ver en la siguiente sección, esto ha empezado a cambiar desde el año 2020.

En los últimos años, ha habido un aumento exponencial en el uso de criptoactivos por parte del ciudadano de a pie, debido a que las barreras de acceso son muy bajas, es tan fácil como descargar una aplicación en un Smartphone y empezar a operar con criptoactivos, sin tener la más mínima idea de qué se trata.

Los usuarios se han visto atraídos a invertir, entre otras cosas, por las promesas de ganancias rápidas, el aumento de los precios del Bitcoin y de otras criptomonedas que alcanzaron su precio récords en 2021⁴⁴⁰, impulsado en parte por la pandemia de la de la COVID-19⁴⁴¹. Lógicamente, esto ha derivado en un aumento de los fraudes y ataques de piratería, lo que los convierte en un objetivo obvio, ya que donde hay fuertes sumas de dinero ahí estarán los estafadores.

Entre los riesgos más comunes para los consumidores encontramos:

- i. Asimetría de la información entre los emisores de criptoactivos y los consumidores⁴⁴².
- ii. Manipulación del mercado.
- iii. Información engañosa y opacidad.
- iv. Explotación (*exploits*) de los Smart Contracts⁴⁴³.

⁴⁴⁰ LANE, M. (2022). "Shutterstock Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself". Disponible en: <https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027> (fecha de consulta: 15 de septiembre de 2022).

⁴⁴¹ AKHTARUZZAMAN, M., BOUBAKER, S., NGUYEN, D. K., & RAHMAN, M. (2022). "Systemic risk-sharing framework of cryptocurrencies in the COVID-19 crisis2. *Finance research letters*. Disponible en: https://www.sciencedirect.com/science/article/pii/S154461232200099X#cit_3 (fecha de consulta: 1 de septiembre de 2022).

⁴⁴² U.S. DEPARTMENT OF THE TREASURY (2022). *Crypto-Asset...*, Op. Cit., p. 26.

⁴⁴³ CHIA, V., HARTEL, P., HUM, Q., MA, S., PILIOURAS, G., REIJSBERGEN, D., VAN STAALDUINEN, M. & SZALACHOWSKI, P. (2018). "Rethinking blockchain security: Position paper", *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber,*

- v. Piratería del sitio web donde se intercambian o custodian los criptoactivos por fallas en la seguridad informática. Recordemos que la mayoría de estas aplicaciones son de código abierto (desarrollo de *software* colaborativo), por lo que está visible para todos, lo que implica que cualquiera puede ver las posibles fallas y explotar las vulnerabilidades.
- vi. Falta de experiencia técnica e infraestructura débil⁴⁴⁴ de las empresas que operan en este sector.
- vii. De igual forma, puede ser común que estas compañías quiebren y desaparezcan sin devolver las inversiones a los usuarios. Sin embargo, muchas veces no es necesario que el proyecto se declare en “insolvencia” para desaparecer. Por ejemplo, el fraude conocido como “tirón de alfombra”, bastante recurrente en DeFi y en el ecosistema de los NFT. Se trata de una estafa en la cual los desarrolladores de un proyecto emiten un token para atraer inversores, para luego huir con los fondos recaudados. Una vez esto sucede, el precio del criptoactivo se desploma y los inversores de ese proyecto ya no lo pueden cambiar por monedas más estables o dinero Fiat, porque su precio está en cero⁴⁴⁵.

La arquitectura técnica de gran parte de las cadenas de bloques limita en su arquitectura los mecanismos de reversión en caso de que las transacciones sean fraudulentas, erróneas o accidentales. Lo que equivale y, quizás sea lo peor es que, este ecosistema tiende a culpar y trasladar la responsabilidad al consumidor. Como mencionó acertadamente el fundador de Dogecoin “si pierdes la contraseña, tu culpa, si eres víctima de una estafa, tu culpa”. Afirmaciones como el “código es ley”, no es más que intento de eximir de responsabilidades a los responsables, tal como lo ha subrayado WALCH “el término «descentralizado» funciona en efecto como un escudo de responsabilidad para

Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData), p. 1274. Disponible en: <https://ieeexplore.ieee.org/document/8726738/authors#authors> (fecha de consulta: 23 de septiembre de 2022).

⁴⁴⁴ MARKETS AND MARKETS. (2021). *Crypto Asset Management Market by Solution (Custodian and Wallets), Application Type (Web-based and Mobile-based), End User (Individuals and Enterprises (Institutions (BFSI, Hedge Funds), Retail and eCommerce))*, and Region - Global Forecast to 2026. Disponible en: <https://www.marketsandmarkets.com/requestsampleNew.asp?id=201925303> (fecha de consulta: 1 de julio de 2022).

⁴⁴⁵ DI PAULA, R. (2022). “¿Cómo funciona el esquema de estafas “rug pull” en el mundo de las criptomonedas?” Disponible en: <https://es.cointelegraph.com/news/how-does-the-rug-pull-work-with-cryptocurrencies> (fecha de consulta: 16 de septiembre de 2022).

quienes operan los sistemas (desarrolladores y mineros), creando lo que yo llamo un «Velo de Descentralización», ello significa este velo actúa de manera similar a al velo corporativo de las sociedades de responsabilidad limitada, pero sin ningún tipo de obligaciones”⁴⁴⁶, pues aún en este tipo de sociedades los accionistas tienen responsabilidades.

3. Implicaciones de la centralización en la protección de los consumidores.

La descentralización y democratización son un mito, puede que un principio esa haya sido la intención de SATOSHI NAKAMOTO, pero esa no es la realidad de hoy día. Lo que hay es almacenamiento distribuido, pero el poder está en mano de unos pocos. Un pequeño grupo de mineros controla la red, como en el caso de Bitcoin o Ethereum, lo que significa que los mineros (o validadores) son quienes deciden qué transacciones pueden hacer parte de un bloque y qué transacciones han de quedar excluidas. En este sentido, los mineros actúan como intermediarios.

En Bitcoin, el 0,1% de los mineros son responsables de la mitad de toda la producción minera⁴⁴⁷, y aunque se piense que al inicio esto no era así, un reciente estudio publicado en junio de 2022 demuestra que la red de Bitcoin nunca ha sido descentralizada, ni siquiera en sus inicios. La investigación demuestra que entre el 3 de enero de 2009 (fecha del primer bloque extraído) y el 9 de febrero de 2011 (cuando el bitcoin alcanzó la paridad con el dólar), la mayoría de los bitcoins, fueron extraídos por 64 agentes, quienes, a pesar de no conocerse, actuaron en interés del colectivo y se negaron a realizar un ataque del 51%, pudiendo haberlo hecho, ya que contaban con más de la mitad de la potencia minera de ese momento⁴⁴⁸. Es más, el cliente de *software* de esta criptomoneda, Bitcoin Core, también está centralizado, aunque es de código abierto, en realidad el *software* que está para su descarga, es mantenido y desarrollado por un pequeño grupo de desarrolladores. Si bien los desarrolladores externos pueden sugerir cambios mediante las

⁴⁴⁶ WALCH, A. (2019). “Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems”, *Chapter in Crypto Assets: Legal and Monetary Perspectives*, pp. 1 y 26. Disponible en SSRN: <https://ssrn.com/abstract=3326244> (fecha de consulta: 10 de agosto de 2022).

⁴⁴⁷GALLOWAY, S. (2022). “The False Promise of Web3”. Disponible en: <https://marker.medium.com/the-false-promise-of-web3-7e6c1a00d4be> (fecha de consulta: 18 de septiembre de 2022).

⁴⁴⁸ BLACKBURN, A., HUBER, C., ELIAZ, Y., SHAMIM, M. S., WEISZ, D., SESHADRI, G., KIM, K., HANG, S. & AIDEN, E. L. (2022). “Cooperation among an anonymous group protected Bitcoin during failures of decentralization”. Disponible en: <https://arxiv.org/abs/2206.02871> (fecha de consulta: 16 de septiembre de 2022).

propuestas de mejora de Bitcoin (BIP), es el pequeño grupo, quienes conservan la potestad sobre si se realizan o no esos cambios⁴⁴⁹. El control del grupo, centraliza, por tanto, las decisiones que se adoptan en la cadena de bloques, lo que no es sino toda una centralización del poder en toda regla.

En el caso de Ethereum, la centralización incluso logró que la recuperación de los fondos robados en el ataque a PolyNetwork⁴⁵⁰, un proyecto DeFi, que tiene por objetivo la interoperabilidad entre cadenas de bloques. Concretamente, el ataque se dio el 10 de agosto de 2022, estableciéndose como uno de los mayores robos de criptomonedas, pues los hackers se llevaron alrededor de 610 millones de dólares de 3 Blockchain diferentes⁴⁵¹. Como respuesta, PolyNetwork a través de su cuenta de Twitter llamó a todos los mineros, casas de cambio de criptomonedas, y Blockchains afectadas, para que incluyesen en su lista negra los tokens provenientes de las direcciones involucradas en el ataque⁴⁵². Este acorralamiento hizo que el pirata no pudiese escapar con el dinero robado y que al final optara por devolverlo. Aunque los fondos robados se recuperaron y el fin pudiera ser noble, esta acción dejó en evidencia la coordinación y concentración de poder que pueden llegar a tener ciertas cadenas de bloques y la inseguridad cibernética a la que se exponen los inversores de un proyecto que tiene comprometido grandes sumas de dinero.

Para que una persona adquiera criptomonedas, deberá comprarlas, intercambiarlas o extraerlas. Usualmente, tendrá que comprarlas con dinero Fiat en una plataforma de intercambio de criptomonedas y, para custodiar los fondos, necesitará de un monedero. Dada la complejidad técnica o la inseguridad que puede suponer autocustodiar el dinero, los consumidores optan por confiar en terceros para hacerlo, ya que es más fácil confiar en un intermediario centralizado que tener que comprender cómo funcionan estos sistemas. Generalmente, cuando los consumidores emplean *exchanges*, en realidad no están usando una Blockchain, por lo tanto, no se benefician de las formas de protección

⁴⁴⁹ MAGNUSON, W. (2020). *Blockchain democracy: Technology, law and the rule of the crowd*, Cambridge University Press, p. 45.

⁴⁵⁰ Véase “PolyNetwork”. (Sin fecha). “ <https://www.poly.network/#/> (fecha de consulta: 12 de septiembre de 2022).

⁴⁵¹ JAGATI, S. (2021). “El hackeo de PolyNetwork expone los fallos de DeFi, pero la comunidad acude al rescate”. Disponible en: <https://es.cointelegraph.com/news/poly-network-hack-exposes-defi-flaws-but-community-comes-to-the-rescue> (fecha de consulta: 12 de septiembre de 2022).

⁴⁵² Véase <https://twitter.com/PolyNetwork2/status/1425073987164381196>

de estas, ya que en realidad no tienen billeteras, sino, cuentas dentro de la billetera de una gran corporación⁴⁵³, como lo puede ser Binance o Coinbase. No obstante, no existe un fondo de garantía de depósito, como en la Unión Europea, que en caso que de que un banco se declare en insolvencia, los consumidores cuentan con un límite de protección de 100 mil euros por depositante, que evita que los ahorradores quiebren junto con el banco, así como tampoco hay un supervisor que rastree o controle transacciones sospechosas para detener una estafa o pirateo. Es decir, que, si una plataforma de intercambio o una billetera fracasa, algo que no es extraño en este ecosistema, no habrá ningún mecanismo de protección para cubrir esas pérdidas.

Estas empresas, generalmente no cumplen con la legislación aplicable en materia de protección a los consumidores, tienen la potestad de gestionar y controlar el dinero de los inversores, como a bien tengan, incluso con periodos de bloqueo de fondos. Recientemente, el 14 de junio de 2022, Celsius, una empresa de préstamos de criptomonedas, que, por cierto, ya se declaró en bancarrota, congeló los retiros, intercambios y transferencias, apelando a “condiciones de mercado extremas”⁴⁵⁴ para proteger la liquidez de la plataforma.

La centralización de las plataformas de intercambio de criptoactivos y las billeteras actúan como un punto único de fallo, es por esta razón que los ataques criminales se han centrado en aprovecharse de las vulnerabilidades de estas plataformas⁴⁵⁵, así lo confirma la larga e inagotable lista de ataques a estos sitios por valor de enormes sumas de dinero. Por ejemplo, podemos destacar algunos hackeos famosos, como el de Mt. Gox, considerado en su momento como la plataforma de intercambio de criptomonedas más grande del mundo. En 2014, un ataque pirata les hizo perder alrededor de 350 millones de dólares en Bitcoin⁴⁵⁶. A los pocos días del incidente la plataforma

⁴⁵³ RUSHKOFF, D. (2022). “What? Your Assets at Coinbase are Not Safe?”. Disponible en: <https://rushkoff.medium.com/what-your-assets-at-coinbase-are-not-safe-3ad20708a888> (fecha de consulta: 12 de septiembre de 2022).

⁴⁵⁴ PEREZ, H. (2022). “Servicio de criptompréstamos Celsius pausa los retiros citando “condiciones extremas del mercado”. Disponible en: <https://www.diariobitcoin.com/criptomonedas/servicio-criptoprestamos-celsius-pausa-retiros-cita-condiciones-extremas-mercado/> (fecha de consulta: 15 de agosto de 2022).

⁴⁵⁵ SAI, A. R., BUCKLEY, J., FITZGERALD, B., & LE GEAR, A. (2021). “Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*”, Vol. 58, No. 4. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0306457321000844#b37> (fecha de consulta: 12 de septiembre de 2022).

⁴⁵⁶ VELASCO, J. (2014). “Mt.Gox y su hundimiento: pérdidas millonarias para unas de las referencias de Bitcoin”. Disponible en: <https://hipertextual.com/2014/02/hundimiento-mt-gox> (fecha de consulta: 12 de septiembre de 2022).

cerró dejando a 20 mil usuarios afectados que a día de hoy aún siguen esperando el reembolso de lo invertido⁴⁵⁷. Asimismo, llama la atención el hackeo a Coinchek en 2018, en el cual se perdieron alrededor de 535 millones de dólares en Nem (una de las criptomonedas más populares de Japón⁴⁵⁸), así como el atraco en diciembre de 2021 a BitMart por valor de 200 millones de dólares⁴⁵⁹. Recientemente, en marzo de 2022, la plataforma de criptomonedas Ronin Network sufrió un robo por valor de 620 millones de dólares en Ether⁴⁶⁰.

Un informe publicado enero de 2022 por CHAINALYSIS⁴⁶¹, reveló que los delitos basados en criptoactivos alcanzaron un nuevo máximo récord en 2021. Las direcciones ilícitas recibieron 14.000 millones de dólares a lo largo de 2021, frente a los 7.800 millones de dólares del año 2020. De esta cifra, aproximadamente de 3.200 millones de dólares corresponden a robos perpetrados por hackeos, cinco veces más de lo que se robaron en 2020. Estos robos han sido el resultado de violaciones de seguridad que tienen por objetivo obtener las claves privadas de las víctimas, las cuales pueden adquirirse mediante *phishing*, *keylogging*⁴⁶², ingeniería social y otras técnicas.

No obstante, a pesar de que los ataques de criptomonedas tenían como objetivo principal las plataformas de intercambio de criptoactivos, esta tendencia cambió desde la pandemia de la COVID-19, pues de los fondos robados en 2021, aproximadamente 2300

⁴⁵⁷ “¿Qué es Mt Gox?” (2022). Disponible en: <https://academy.bit2me.com/que-es-mt-gox/> (fecha de consulta: 17 de septiembre de 2022).

⁴⁵⁸ PASTOR, J. (2018). “Coincheck sufre el mayor robo de criptodivisas de la historia, 535 millones de dólares en NEM”. Disponible en: <https://www.xataka.com/criptomonedas/coincheck-detiene-operaciones-de-retirada-de-criptodivisas-y-los-usuarios-estan-empezando-a-temer-lo-peor> (fecha de consulta: 17 de septiembre de 2022).

⁴⁵⁹ SHUMBA, C. (2021). “BitMart suspende la retirada de dinero tras sufrir un ciberataque: los delincuentes roban 173 millones en criptomonedas con una clave privada”. Disponible en: <https://www.businessinsider.es/bitmart-sufre-ciberataque-sustraen-173-millones-criptomonedas-976183> (fecha de consulta: 12 de septiembre de 2022).

⁴⁶⁰ HOWELL, P. (2022). “575 millones de euros: un golpe rutinario para los ladrones de criptodivisas”. Disponible en: <https://www.technologyreview.es/s/14155/575-millones-de-euros-un-golpe-rutinario-para-los-ladrones-de-criptodivisas> (fecha de consulta: 14 de septiembre de 2022).

⁴⁶¹ CHAINALYSIS. (2022). *The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime*. Disponible en: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf> (fecha de consulta: 8 de agosto de 2022), CHAINALYSIS. (2022). “Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity”. Disponible en: <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/> (fecha de consulta: 8 de agosto de 2022) y CHAINALYSIS. (2021). “The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs”. Disponible en: <https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/> (fecha de consulta: 8 de agosto de 2022).

⁴⁶² Según AVAST. (2022). “¿Qué son los keyloggers y cómo funcionan?” Disponible: <https://www.avast.com/es-es/c-keylogger> (fecha de consulta: 6 de febrero de 2023), son “un tipo de *software* malicioso que registra todas las pulsaciones de teclas que realice en el ordenador.

millones de dólares, es decir, el 72% fueron robados de protocolos DeFi. El informe también destaca que las pérdidas de dinero en su mayoría no obedecen a ataques piratas, sino más bien a delitos relacionados con estafas de inversión, específicamente de tirón de alfombra, la estafa referente de DeFi, que representa el 37% de todos los ingresos por estafas. De hecho, advierte CHAINALYSIS que el 90% del valor total perdido en esta modalidad se atribuye a una sola plataforma, Thodex, una casa de cambio de criptomonedas de origen turco.

No obstante, según CHAINALYSIS en 2022 las estafas de los protocolos DeFi han disminuido. Según un informe publicado a mitad de año por la empresa de análisis de cadena de bloques, los ingresos totales por estafa hasta julio de 2022 ascienden a 1.6 mil millones de dólares, un 65% menos para el mismo periodo de 2021. Sin embargo, advierte el informe que esta disminución puede estar relacionada con la caída de los precios de las criptomonedas, puesto que menos personas caen en este tipo de estafas, pues con la disminución de los precios de los activos, las enormes ganancias prometidas son menos atractivas para las potenciales víctimas. También se ha relacionado con que hay menos presencia de usuarios nuevos e inexpertos, ya que cuando hay tendencia bajista no se ven atraídos por la exageración y la promesa de ganancias rápidas. Pero mientras que las estafas han disminuido, los ataques han aumentado, pues hasta julio de 2022 se robaron 1900 millones de dólares, en comparación con aproximadamente 1200 millones de dólares en el mismo periodo del año anterior, aunque el blanco de ataque continúa siendo los proyectos DeFi⁴⁶³.

II. ADVERTENCIAS A NIVEL EUROPEO

Las autoridades de supervisión financiera europea han expuesto su preocupación por los riesgos que supone operar con criptoactivos, por ello, de cara a mitigar un poco esos peligros, han emitido advertencias para alertar sobre los riesgos financieros que pueden suponer operar con criptoactivos. En este apartado, destacaremos las advertencias

⁴⁶³ CHAINALYSIS. (2022). “Mid-year Crypto Crime Update: Illicit Activity Falls With Rest of Market, With Some Notable Exceptions”. Disponible en: <https://blog.chainalysis.com/reports/crypto-crime-midyear-update-2022/> (fecha de consulta: 12 de septiembre de 2022).

más relevantes que han hecho los supervisores europeos para intentar detener estas prácticas y luego destacaremos los avisos que se han emitido a nivel español.

Las autoridades que han alertado forman parte del Sistema Europeo de Supervisión Financiera (SESF), compuesto a su vez por la Autoridad Europea de Valores y Mercados (ESMA), la Autoridad Bancaria Europea (ABE) y la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ). También incluye a la Junta Europea de Riesgo Sistémico (JERS), y al Comité Mixto de las Autoridades Europeas de Supervisión y las autoridades nacionales de supervisión⁴⁶⁴. De ellas, debemos destacar a la ABE, una autoridad independiente de la UE que trabaja para garantizar un nivel efectivo y coherente de regulación y supervisión prudencial en todo el sector bancario europeo para lograr la estabilidad financiera en la Unión Europea, así como la integridad, la eficiencia y el correcto funcionamiento del sector bancario.

En relación con los riesgos que pueden suponer las criptomonedas, la ABE advierte por primera vez en diciembre de 2013⁴⁶⁵ avisando sobre el peligro financiero que puede suponer a los consumidores, tanto la adquisición, como el acopio y las transacciones comerciales de estas criptomonedas, que estaban ganando una popularidad cada vez mayor entre la población. Así, destacan la ausencia de un marco regulatorio que proteja al consumidor contra las pérdidas, en caso de inviabilidad o cierre de las plataformas que operan con estas criptomonedas.

De igual manera, definen las monedas virtuales como “una modalidad de dinero digital no regulado, que no se emite por un banco central y que puede servir como método de pago”. De entrada, esta descripción es, a todas luces, una advertencia al respecto del escaso respaldo financiero de las mismas en caso de surgir cualquier contratiempo para el consumidor.

⁴⁶⁴ Véase https://www.eba.europa.eu/languages/home_es

⁴⁶⁵ AUTORIDAD BANCARIA EUROPEA. (2013). “Aviso a los consumidores sobre las monedas virtuales”. Disponible en: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598420/00742a76-9c02-46c5-a615-40105fe75b94/EBA_2013_01030000_ES_TRA1_Vinay.pdf?retry=1 (fecha de consulta: 4 de agosto de 2022).

Respecto a la adquisición e intercambio de divisas, destacan los riesgos asociados a las plataformas digitales de intercambio y almacenamiento de criptodivisas: falta de regulación, posibilidad de cierre o quedar inutilizadas por un ataque informático, sin que ningún organismo responda por ello.

De tal manera, advierten de que, en caso de que una de estas plataformas de intercambio pierda su dinero por uno u otro motivo, no hay ningún sistema a modo de garantía de depósito. Lo mismo ocurre con las carteras digitales, las cuales no solo no son inmunes al pirateo (existiendo la posibilidad de que su dinero sea sustraído sin ningún tipo de respaldo), sino que, en caso de perder las claves de acceso, no habrá manera de recuperar el dinero en ellas depositado, sin que exista la posibilidad de recuperar dicha contraseña por otro medio. En el mismo orden de ideas, destacan que las transacciones realizadas con criptomonedas no están protegidas por los derechos de reembolso respaldados por la legislación comunitaria, sin la posibilidad de revertir un pago erróneo o fraudulento.

Asimismo, tratan de concienciar sobre la elevada volatilidad de las criptomonedas (riesgo de pérdidas bruscas) y el riesgo de su empleo en actividades delictivas, como puede ser el blanqueo de capitales, existiendo la posibilidad de que la plataforma en la que el consumidor ha invertido su dinero sea bloqueada por las autoridades debido a alguna actividad delictiva, perdiendo así el acceso a su inversión. Por último, destacan que las criptomonedas pueden estar sujetas a obligaciones fiscales, siendo responsabilidad del usuario examinar cuáles son las que rigen en su caso particular.

Como recomendaciones para minimizar estos riesgos, sugieren al consumidor estar bien informado de las características de la criptodivisa que va a adquirir, su modelo de negocio, la transparencia y la percepción pública de las plataformas de intercambio que emplee, así como no acumular grandes cantidades de dinero en una sola cartera.

Este aviso fue a todas luces insuficiente, de manera que nuevas advertencias al respecto se emitieron por parte de la ABE en julio de 2014 y agosto de 2016. Sin embargo, no fue hasta febrero de 2018 que se emite un nuevo comunicado, esta vez por parte de las

3 entidades fundamentales que integran el Sistema Europeo de Supervisión Financiera: ESMA, ABE y AESPJ⁴⁶⁶.

En este nuevo comunicado, vuelve a insistirse en la ausencia de respaldo por un activo tangible por parte de las criptomonedas, agravándose la preocupación de estos organismos debido al auge que están recibiendo las mismas a modo de especulación, desconociendo gran parte de los consumidores el alto riesgo de pérdida de sus activos al que están sometidos, por primera vez se comenta el riesgo evidente de convertirse en una burbuja al que están sometidas las criptomonedas. Asimismo, a la fecha de publicación de este artículo, aún no había entrado en vigor ninguna legislación, de manera que seguían sin estar reguladas por la UE, como ya se advirtió en 2013.

A las advertencias ya descritas en 2013, agregan que, la falta de opciones de salida de las monedas virtuales, esto es, la posibilidad de no poder intercambiarlas por dinero tradicional; la falta de transparencia en sus precios, es decir, la posibilidad de no recibir un precio justo en las transacciones; las interrupciones operativas (periodos en los que las plataformas no permiten comprar o vender criptomonedas, pudiendo suponer una pérdida para el interesado) y la información engañosa en torno a las criptodivisas. Como medidas de seguridad, se añade que la compra de monedas virtuales a una empresa regulada por servicios financieros, no reduce los múltiples riesgos asociados al intercambio de criptodivisas.

En marzo de 2021, se realiza una nueva advertencia conjunta⁴⁶⁷, destacando de nuevo la falta de regulación, dado que, volviendo al punto de la información engañosa, gran parte de los consumidores creían que las criptomonedas estaban siendo reguladas por la propuesta legislativa de septiembre de 2020 por parte de la Comisión Europea. Sin embargo, esta aún no había adquirido el carácter de ley y, por tanto, no ha entrado en vigor.

⁴⁶⁶ AUTORIDAD EUROPEA DE VALORES Y MERCADOS, AUTORIDAD BANCARIA EUROPEA & AUTORIDAD EUROPEA DE SEGUROS Y PENSIONES DE JUBILACIÓN. (2018). “ESMA, ABE y AESPJ advierten a los consumidores de los riesgos de las monedas virtuales”. Disponible en: <https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/Noticias%20Ultima%20Hora/EBAVirtualCurrenciesES.pdf> ((fecha de consulta: 4 de agosto de 2022).

⁴⁶⁷ AUTORIDAD BANCARIA EUROPEA. (2021).” Crypto-assets: ESAs remind consumers about risks”. Disponible en: <https://www.eba.europa.eu/financial-innovation-and-fintech/publications-on-financial-innovation/crypto-assets-esas-remind-consumers-about-risks> (fecha de consulta: 8 de agosto de 2022).

Finalmente, en 2022⁴⁶⁸, en un nuevo comunicado conjunto, destacan el repunte de las criptomonedas asociado a la información y publicidad engañosa que están recibiendo las criptomonedas por parte de las redes sociales e *influencers*. Asimismo, instan a los usuarios a que, en caso de querer asumir los riesgos asociados a esta actividad, consulten las listas negras de las autoridades nacionales pertinentes.

A los riesgos anunciados en artículos anteriores, añaden el repunte de actividades maliciosas en torno a las criptomonedas, como el phishing; problemas de seguridad y casos de manipulación del mercado. De igual manera, extienden estas advertencias a nuevas tecnologías como son los NFTs o DeFi.

1. Advertencias por parte de autoridades españolas

De igual forma, a nivel español han sido emitidos comunicados en la misma línea por parte del Banco de España y la Comisión Nacional del Mercado de Valores (CNMV). En concreto, emitieron un primer comunicado en el año 2018⁴⁶⁹, en el cual advirtió no solo en relación con las criptomonedas, sino también sobre las Ofertas Iniciales de Criptomonedas (ICOs), que hace referencia a la emisión tanto de criptomonedas como de los “Tokens”, ya sean “*security tokens*” (participación en el aumento de valor futuro) o “*utility tokens*” (acceso directo a un servicio o producto, poseyendo también un carácter de posible revalorización/negocio).

A grandes rasgos, recoge las mismas aportaciones que previamente los organismos comunitarios emitieron en torno a este tema, recopilando la misma definición de las criptomonedas y haciendo énfasis en su fuerte componente de variabilidad y especulativo a modo de burbuja, así como en el alto riesgo de fraude. Entre ellos, destacan el carácter global del fenómeno, de manera que al no encontrarse en gran cantidad de

⁴⁶⁸ AUTORIDAD EUROPEA DE VALORES Y MERCADOS, AUTORIDAD BANCARIA EUROPEA & AUTORIDAD EUROPEA DE SEGUROS Y PENSIONES DE JUBILACIÓN. (2022). “Los reguladores financieros de la UE advierten a los consumidores sobre los riesgos de los cryptoactivos”. Disponible en: <https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/InformacionInteres/EBA/Arc/Fic/2022-03-14-notaconjuntaautoridadesUE-crypto.pdf> (fecha de consulta: 4 de agosto de 2022).

⁴⁶⁹ BANCO DE ESPAÑA. (2018). “Comunicado conjunto de la CNMV y del Banco de España sobre “criptomonedas” y “ofertas iniciales de criptomonedas” (ICOs)”. Disponible en: https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07.pdf (fecha de consulta: 4 de agosto de 2022).

ocasiones las plataformas de intercambio, carteras o ICOs en España, pueden quedar fuera del ámbito de actuación de las autoridades españolas.

Así, instan a los inversores a que, en caso de estar dispuestos a asumir los riesgos, reciban información adecuada al respecto. Se manifiesta una preocupación en torno al auge tanto de las criptomonedas, como de los ICOs. Cabe destacar que, a la fecha de emisión de dicho comunicado, ninguna criptomoneda, ni ICO, había sido registrada o autorizada por las autoridades españolas, de manera que, al igual que ocurre a nivel comunitario, no reciben ninguna de las garantías provistas por las mismas. Al respecto de las ICOs en particular, se remiten al comunicado de la International Organization of Securities Commissions (IOSCO) de 2018, en el cual ya se realizan advertencias en torno a la alta volatilidad y riesgo de fraude de las mismas.

En 2021⁴⁷⁰, nuevamente el Banco de España junto a la CNMV realizaron un nuevo comunicado, abarcando los mismos puntos que el comunicado anterior, pero en este caso añadiendo énfasis a temas como la elevada complejidad que suponen estas inversiones para el inversor medio (no experto), la susceptibilidad a la manipulación de los precios en el mercado y el escaso valor que presentan los criptoactivos como método de pago (sin que sea obligatorio recibirlos por parte de los comercios).

En 2022⁴⁷¹, se emitió un último comunicado, esta vez respaldado además por la Dirección General de Seguros, remitiéndose a las advertencias previas realizadas por los organismos comunitarios, añadiendo además información correspondiente a la Circular 1/2022⁴⁷² (en adelante la Circular), que busca regular las campañas publicitarias en torno a los criptoactivos de inversión financiera, su contenido y su formato, así como lograr que la información al respecto sea lo suficientemente completa como para que el consumidor

⁴⁷⁰ BANCO DE ESPAÑA & COMISIÓN NACIONAL DEL MERCADO DE VALORES. (2021). “Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión”

Disponible en: <https://www.cnmv.es/portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D> (fecha de consulta: 4 de agosto de 2022).

⁴⁷¹ BANCO DE ESPAÑA, COMISIÓN NACIONAL DEL MERCADO DE VALORES & DIRECCIÓN GENERAL DE SEGUROS Y FONDOS DE PENSIONES (2022). “Comunicado conjunto del Banco de España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos”. Disponible en:

https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/22/presbe2022_19.pdf (fecha de consulta: 4 de agosto de 2022).

⁴⁷² España. Circular 1/2022, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversión. Boletín Oficial del Estado, 10 de enero de 2022.

sea consciente de los riesgos de su inversión, y al Real Decreto-ley 7/2021⁴⁷³, que pone en funcionamiento un Registro en el cual deben inscribirse aquellos que ofrezcan servicios de intercambio de criptomonedas por moneda de curso digital, así como las carteras digitales, a fin de lograr una prevención del blanqueo de capitales y financiación del terrorismo.

2. Tratamiento de los criptoactivos en España

El desarrollo normativo en España para la protección del consumidor en este escenario solo regula cuestiones relativas a la publicidad, sin embargo, estos intentos y acercamientos no son suficientes para asegurar su protección de cara a los riesgos que supone operar con criptoactivos. Leyes generales como TRLGDCU⁴⁷⁴ y LCG⁴⁷⁵ no ofrecen soluciones a problemas típicos relacionados con la compra, venta, negociación y custodia de criptoactivos. Ahora bien, una vez que MiCA entre en vigencia, estas leyes van a complementar y reforzar las medidas de protección, no obstante, en esta sección no entraremos en detalle sobre estas cuestiones, ya que están por fuera del alcance de este capítulo. En este sentido, no es conveniente mantener esta regulación en una zona gris o hacerlo por analogía con las regulaciones existentes, pues esta tecnología presenta unas particularidades únicas que requieren respuestas concretas y conjuntas, no solo a nivel europeo, sino global.

2.1 Competencias de la CNMV en materia de publicidad

Si bien España no cuenta con un régimen jurídico que regule de forma específica a los criptoactivos, la CNMV elaboró a comienzos de 2022 una circular que tiene por objetivo el desarrollo de reglas aplicables a la actividad publicitaria sobre criptoactivos y delimitar el ámbito objetivo y subjetivo de aplicación⁴⁷⁶. Esta circular es consecuencia directa del Real Decreto-ley 5/2021, de medidas extraordinarias de apoyo a la solvencia

⁴⁷³ España. Real Decreto-ley 7/2021 de prevención del blanqueo de capitales y de la financiación del terrorismo. *Boletín Oficial del Estado*, 27 de abril de 2021.

⁴⁷⁴ España. Real Decreto 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. *Boletín Oficial del Estado*, 16 de noviembre de 2007.

⁴⁷⁵ España. Ley 7/1998, sobre condiciones generales de la contratación. *Boletín Oficial del Estado*, 13 de abril de 1998.

⁴⁷⁶ Artículo 1 de la Circular.

empresarial en respuesta a la pandemia de la COVID-19 que, en aras de reforzar el marco regulatorio de la protección del inversor, introdujo un nuevo artículo a la Ley del Mercado de Valores (artículo 240 bis⁴⁷⁷), el cual le otorga a la CNMV “competencias con el fin de sujetar a control administrativo la publicidad de criptoactivos” y otros instrumentos financieros que se ofrecen como objeto de inversión y que no están bajo el ámbito de aplicación de la Ley del Mercado de Valores⁴⁷⁸.

A pesar de que la CNMV venía advirtiendo en diferentes comunicados sobre los riesgos de operar con esta clase de activos, la pandemia propició una oleada de publicidad que hizo que muchos pequeños inversores invirtieran en estos mercados. Las empresas del mundo cripto se sirven en muchas ocasiones *influencers* y celebridades, para dar la impresión de que no se trata de una publicidad, sino de una invitación para hacer parte de algo grande a los que ellos pertenecen. No obstante, ese “algo” es una inversión arriesgada, en la que probablemente perderán su dinero.

Esta circular dota de poderes y herramientas a la CNMV para que supervise la publicidad de criptoactivos, siempre y cuando, estos no tengan la consideración de activos financieros según la Ley del Mercado de Valores⁴⁷⁹. En este sentido, la Circular se erige como una de las primeras normas con relación a los criptoactivos en la legislación española. Si bien el objetivo de la circular es regular determinados aspectos relacionados con la publicidad, brinda la siguiente definición de criptoactivos ““representación digital de un derecho, activo o valor que puede ser transferida o almacenada electrónicamente, utilizando tecnologías de registro distribuido u otra tecnología similar”⁴⁸⁰. Menciona

⁴⁷⁷ “Se añade un nuevo artículo 240 bis, con la siguiente redacción: «Artículo 240 bis. La CNMV podrá someter a autorización u otras modalidades de control administrativo, incluida la introducción de advertencias sobre riesgos y características, la publicidad de criptoactivos u otros activos e instrumentos presentados como objeto de inversión, con una difusión publicitaria comparable, aunque no se trate de actividades o productos previstos en esta Ley. La CNMV desarrollará mediante circular, entre otras cuestiones, el ámbito subjetivo y objetivo y las modalidades concretas de control a las que quedarán sujetas dichas actividades publicitarias

A estos efectos resultará de aplicación lo dispuesto en el segundo párrafo del artículo 240 de esta Ley.»”.

⁴⁷⁸ CNMV. (2022). “publicidad de criptoactivos”. Disponible en: <https://www.cnmv.es/portal/inversor/Publicidad-Criptoactivos.aspx> (fecha de consulta: 10 de octubre de 2022).

⁴⁷⁹ España. Real Decreto Legislativo 4/2015, por el que se aprueba el texto refundido de la Ley del Mercado de Valores. *Boletín Oficial del Estado*, 23 de octubre de 2015

⁴⁸⁰ Artículo 3.e de la Circular.

MORALES y otros, que esta sería la única definición en el derecho local relativa a los criptoactivos⁴⁸¹.

2.1.1 Ámbito de aplicación

i. Ámbito Objetivo

El ámbito objetivo de la Circular se circunscribe a la actividad publicitaria⁴⁸² que sean objeto de inversión. En este sentido, la circular entiende como actividad publicitaria “toda publicidad dirigida a inversores o potenciales inversores en España en la que se ofrezcan o se llame la atención, de forma implícita o explícita, sobre criptoactivos como objeto de inversión”. Además, establece las siguientes presunciones: por un lado, se presume que un criptoactivo se ofrece o se llama la atención sobre él, como posible objeto de inversión, cuando se promueva su adquisición o se haga cualquier referencia a su rentabilidad, precio o valor, actuales o futuros, que pudiera sugerir una oportunidad de invertir en dicho criptoactivo, aun cuando eventualmente puedan ser utilizados como medio de cambio. Y por el otro lado, se presume que la actividad publicitaria va dirigida a inversores en España cuando se realice mediante medios físicos, a través de medios de comunicación.

La circular excluye de su ámbito de aplicación objetivo la publicidad sobre: a) criptoactivos que tengan la naturaleza de instrumentos financieros incluidos en el anexo de la Ley del Mercado de Valores, que ya se encuentran regulados por la Circular 2/2020 de la CNMV; b) que por sus características y su naturaleza no sean susceptibles de ser objetos de inversión; c) criptoactivos cuyo único objetivo sea el acceso digital a un producto o servicio, y sea aceptado únicamente por su emisor o un conjunto limitado de proveedores comerciales, con los que el proveedor mantiene una relación contractual, y siempre y cuando no se ofrezcan expectativas de revalorización. Es decir, que constituyan fichas de servicio conforme a MiCA; d) NFTs, cuando representan activos coleccionables, obras con propiedad intelectual o activos con el único fin de ser usados en juegos o competiciones, f) los libros blancos; f) las campañas publicitarias corporativas

⁴⁸¹ MORALES, J.& CHOLVI, F. (2022). “Criptoactivos y sector financiero: revolución en el mercado y retos regulatorios”. Disponible en: https://www.garrigues.com/es_ES/garrigues-digital/criptoactivos-sector-financiero-revolucion-mercado-retos-regulatorios (fecha de consulta: 24 de enero de 2023).

⁴⁸² Artículo 3.1 de la Circular.

que contengan exclusivamente información genérica; g) la documentación o informaciones que se proporcionen en presentaciones dirigidas únicamente a analistas o inversores institucionales; h) las publicaciones que emitan los analistas financieros o comentaristas independientes, que no estén patrocinadas o promocionadas; i) la publicidad sobre seminarios técnicos, cursos y jornadas sobre criptoactivos que en ningún caso fomenten la inversión en los mismos y que no se promocionen de forma gratuita o por un precio simbólico.

ii. Ámbito subjetivo

La Circular somete a su ámbito de aplicación subjetivo a: a) los proveedores de servicios de criptoactivos cuando estos realicen actividades publicitarias sobre los mismos; b) los proveedores de servicios publicitarios y c) cualquier persona, que realice por iniciativa propia o por cuenta de terceros una actividad publicitaria sobre criptoactivos. De la lectura de este punto se desprende que la Circular estaría incluyendo bajo su ámbito de aplicación a los *influencers* y celebridades.

2.1.2 Control de la publicidad

Señala la Circular⁴⁸³ que las campañas publicitarias deberán tener en cuenta la naturaleza y complejidad del producto, las características de los medios de difusión utilizados y el público al que se dirijan. Asimismo, todas las comunicaciones comerciales deberán incluir información sobre los riesgos del producto publicitado, en concreto la siguiente advertencia; “La inversión en criptoactivos no está regulada, puede no ser adecuada para inversores minoristas y perderse la totalidad del importe invertido”, también se tendrá que incluir un enlace a la ubicación de la información adicional con el siguiente texto “Es importante leer y comprender los riesgos de esta inversión que se explican detalladamente en esta ubicación”.

⁴⁸³ Artículo 5 de la Circular.

2.1.3 Supervisión de la actividad publicitaria

Advierten LÓPEZ-LAPUENTE y otros⁴⁸⁴ que la Circular centra el objetivo de las facultades supervisoras de la CNMV en torno a dos regímenes, primero, se exige la comunicación previa a la CNMV de campañas publicitarias, segundo, se faculta a la CNMV para requerir el cese o rectificación de la actividad publicitaria.

En principio, la actividad publicitaria dirigida a inversores no precisa de comunicación previa a la CNMV, a menos que se trate de campañas masivas que se dirijan a más de 100 mil personas. Dicha comunicación deberá hacerse 10 días hábiles antes de su ejecución. Además, la CNMV podrá exigir la comunicación previa a determinados sujetos, a pesar de que no se trate de campañas publicitarias masivas, por el impacto que pudieran tener en el público objetivo. Por otra parte, se les exige a los sujetos obligados mantener un registro con información y documentación respecto a las campañas publicitarias en curso y a las realizadas en los últimos dos años. Este punto es importante, porque en caso de requerimiento por parte de la CNMV, se deberá aportar dicho registro.

En relación con el cese o rectificación de la actividad publicitaria⁴⁸⁵, la CNMV podrá informar a los sujetos obligados los desajustes que considere en su actividad publicitaria y requerir el cese de la publicidad o su rectificación.

2.2 Proyecto de Ley de los Mercados de Valores y de Servicios de Inversión

El pasado 12 de septiembre de 2022 se publicó el Proyecto de Ley de los Mercados de Valores y de los Servicios de Inversión que busca sustituir la actual ley del mercado de valores. Con respecto a los criptoactivos, esta normatividad introduce normas para adaptar la aplicación de MiCA en el ordenamiento jurídico español una vez este se apruebe. Se designa a la CNMV como autoridad competente para sancionar y supervisar la admisión, oferta y admisión a negociación de ciertos criptoactivos que no tengan la consideración de instrumentos financieros, tales como los *utility tokens*. De manera que,

⁴⁸⁴ LÓPEZ-LAPUENTE, L., NIETO, E., SAINZ, B., SEIJO, A. & TEROL, S. (2022) “Non Fungible Tokens (NFTs)”, *Blockchain: aspectos jurídicos de su utilización* (Dirs. VALPUESTA, E. & HERNANDEZ, J.) Ed.: La Ley, Las Rozas, Madrid, p. 174.

⁴⁸⁵ Artículo 6.4 de la circular.

el Banco de España será la autoridad encargada de supervisar, inspeccionar y sancionar a los emisores de ficha de dinero electrónico y las fichas referenciadas a activos.

Asimismo, se incluyen reglas que contemplan el empleo de la tecnología Blockchain “para el registro, compensación y liquidación de valores negociables e instrumentos financieros”⁴⁸⁶. En este sentido, la definición de instrumento financiero incluye aquellos que utilicen la tecnología de registros distribuidos (TRD) o tecnologías similares. De tal manera que, se garantiza la jurídica de los instrumentos financieros cuando empleen la tecnología Blockchain, pues estos quedarían sujetos a las disposiciones de esta nueva normatividad.

III.LA PROTECCIÓN DE LOS CONSUMIDORES Y LA PROPUESTA DE REGLAMENTO

1. Introducción

En aras de proporcionar una respuesta integral al desafío regulatorio de los criptoactivos⁴⁸⁷, la Comisión Europea presentó en septiembre de 2020 la propuesta de Reglamento relativo a los mercados de criptoactivos⁴⁸⁸ (MiCA, por sus siglas en inglés *Markets in Crypto-Assets*). Esta propuesta de reglamento relativa a los mercados de criptoactivos se encuentra, actualmente en negociación en el interior de las instituciones europeas. De hecho, el pasado el 5 de octubre de 2022 fue aprobada por Consejo Europeo, solo falta la aprobación por parte del Parlamento Europeo. De llegar a ocurrir, se espera que entre en vigencia para 2024.

La referida propuesta de Reglamento forma parte de un paquete de finanzas digitales de la Comisión Europea, que incluye además una estrategia de finanzas digitales,

⁴⁸⁶ “Proyecto de nueva Ley de los Mercados de Valores y de los Servicios de Inversión”. (2022)., p. 1. Disponible en: <https://www.uria.com/documentos/circulares/1570/documento/12942/UM-nota.pdf?id=12942&forceDownload=true> (fecha de consulta: 26 de enero de 2023).

⁴⁸⁷ BANCO DE ESPAÑA (2022). *Informe de estabilidad...*, Op. Cit., p. 165

⁴⁸⁸ Reglamento Del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, en adelante la propuesta de Reglamento o MiCA.

una estrategia de pagos de minoristas y una propuesta legislativa, resiliencia operativa digital⁴⁸⁹ (DORA, por sus siglas en inglés).

Advierte MiCA que su objetivo es regular la actividad económica de los criptoactivos, más allá de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Asimismo, busca unificar la legislación, evitar el arbitraje regulatorio y la actual fragmentación del mercado de criptoactivos, debido a las medidas tomadas de forma individual al respecto por cada uno de los estados miembros.

Es importante destacar que, la propuesta de Reglamento regula los criptoactivos que no entran en la categoría de instrumentos financieros, como los *Security Tokens*, ya que estos se encuentran bajo el ámbito de aplicación de MiFID II⁴⁹⁰. Para estos criptoactivos, la Comisión Europea propone un régimen piloto sobre infraestructuras del mercado basadas en la tecnología de registros descentralizados, para que los actores de estos instrumentos experimenten en un entorno seguro, es decir, un entorno de pruebas o *sandbox*⁴⁹¹ que aporte experiencia e información de cara a potenciales modificaciones. Actualmente dicho régimen piloto se encuentra regulado por el Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado. El objetivo último de este organismo consistiría en generar un marco normativo sólido al respecto, que fomente la innovación y que a la vez defienda los intereses de los consumidores, respetando la estabilidad financiera, como señala en la doctrina PASTOR SEMPERE, “En definitiva, su objetivo es garantizar que la legislación de la Unión en materia de servicios financieros se adapte a la era digital y contribuya a

⁴⁸⁹ CONSEJO DE LA UE Y CONSEJO EUROPEO. (2022). “Finanzas digitales”. Disponible en: <https://www.consilium.europa.eu/es/policies/digital-finance/#:~:text=El%20paquete%20tiene%20por%20objeto,consumidores%20y%20la%20estabilidad%20financiera> (fecha de consulta: 16 de octubre de 2022).

⁴⁹⁰ Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE.

⁴⁹¹ MARTÍNEZ, L. M. G. (2021). “Infraestructuras de mercado basadas en tecnología de registro distribuido (TRD): el futuro Régimen Piloto de la UE”, *Revista de derecho del mercado de valores*, No. 29. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=8263989> (fecha de consulta: 28 de septiembre de 2022).

una economía preparada para el futuro que funcione para las personas, incluso permitiendo el uso de tecnologías innovadoras”⁴⁹².

Respecto a fomentar la innovación, cabe destacar que, con esta propuesta, se pretende no solo proteger al consumidor, sino también al empresario y, con ello, lograr un beneficio para la Unión Europea. En este sentido, la existencia de un marco regulador común permitirá a aquellas empresas relacionadas con las criptoactivos ajustarse a una única reglamentación, evitando la multiplicación de sus esfuerzos.

Actualmente, y debido al modelo de negocio global que suponen los criptoactivos, una empresa que quiera instalarse en diversos estados de la UE, deberá ceñirse a las leyes y afrontar los diversos trámites administrativos correspondientes a cada país, lo que implica un sobrecoste para las empresas, en el caso de que exista una regulación que permita su actividad económica de forma controlada en el país de destino.

En este aspecto, una cripto-economía estructurada y regulada desde el punto de vista normativo, común a nivel europeo, aportaría igualmente una mayor seguridad a aquellos consumidores individuales que pretendan adentrarse en esta actividad económica, dado que, para ejercer dicha actividad, se le exigirán una serie de requisitos mínimos a las empresas.

Así, originalmente se plantearon dos posibilidades para la regulación de criptoactivos no contemplados por la legislación vigente de servicios financieros:

- i. Régimen de participación voluntaria en relación con los criptoactivos no regulados: Lo que significaría que los emisores y proveedores de servicios podrían participar voluntariamente en la regulación europea, recibiendo una especie de “pasaporte” que les permitiría operar en el interior de la misma. Aquellos que decidiesen no participar voluntariamente seguirían sin estar regulados o sujetos a las normativas nacionales.

⁴⁹² PASTOR-SEMPERE, C. (2020). “La reconstrucción económica europea y el futuro Reglamento MiCA”. Disponible en: <https://www.legaltoday.com/opinion/articulos-de-opinion/la-reconstruccion-economica-europea-y-el-futuro-reglamento-mica-2020-11-19/> (fecha de consulta: 24 de enero de 2023).

ii. Plena armonización: lo que significaría que todos estarían regulados y obtendrían el “pasaporte de la UE”, de manera que no se aplicarían las reglamentaciones individuales de cada país miembro. Esta segunda opción era la que parecía ser más sensata, dado que permitía un marco de actividad más unificado, contribuyendo asimismo a mantener la cohesión del mercado.

Especial mención merecen las criptomonedas estables, las cuales suponen un especial riesgo a la estabilidad financiera de la UE, al poseer un mayor potencial de expansión entre la población. Por ello, y para favorecer la regulación de las mismas, se consideraron diversas opciones:

Opción 1ª. “Régimen legislativo específico”. Dirigido a afrontar los riesgos que plantean las criptomonedas estables y las criptomonedas estables mundiales. Tomando un enfoque basado en el riesgo, esta opción afrontaría las vulnerabilidades de las *stablecoin* respecto con la estabilidad financiera, con la posibilidad de desarrollar diferentes modelos de negocios de criptomonedas estables.

Opción 2ª. “Regulación de las *stablecoin* en el marco de la Directiva sobre el dinero electrónico”. Esta opción de algún modo establecería una similitud demasiado simplista entre las criptomonedas y el dinero electrónico, dejando en el aire y sin regular diversas posibilidades. La comisión consideró que la combinación de las opciones de esta opción, con la primera era lo más conveniente, pues se reducían los riesgos en relación con la estabilidad financiera.

Opción 3ª. “Medidas destinadas a limitar el uso de las criptomonedas estables en la UE”. Esta opción tendría sentido en la medida en que se asume que el riesgo de las criptomonedas estables para la estabilidad financiera de la UE es mayor a sus potenciales beneficios, sin embargo, esta medida supondría un perjuicio a aquellas criptomonedas ya establecidas y entraría en disputa con uno de los objetivos fundamentales de la normativa, como es la promoción de la innovación tecnológica.

2. Respuesta de MiCA para la protección de los consumidores

Nos proponemos determinar y analizar las medidas de protección al consumidor proporcionadas por el proyecto de reglamento. Para ello, primero delimitaremos el concepto de consumidor y el ámbito de aplicación del futuro Reglamento. Seguidamente, describiremos las clases de criptoactivos que se regulan, así como los proveedores de servicios de criptoactivos y las obligaciones que tienen de cara a la protección al consumidor. Finalmente, delimitaremos las salvaguardas de protección al consumidor propuestas en MiCA, haciendo alusión a los requisitos del libro blanco (*whitepaper*), el derecho de desistimiento, procedimiento de reclamaciones y Prevención del abuso del mercado.

2.1 Concepto de consumidor

Define el Reglamento consumidor como “toda persona física que actúe con fines ajenos a su actividad comercial, empresarial, oficio o profesión”⁴⁹³. Esta es, sin duda una definición de consumidor bastante sencilla y amplia, pues la consideración de consumidor no queda condicionada a requisitos específicos. Advierte en la doctrina LOIS CABALLE que, la propuesta “opta por la inclusión financiera del consumidor al contemplarlo simplemente como adquirente de criptoactivos, sin que sea necesario que haga una compra mínima”⁴⁹⁴.

Por otro lado, la propuesta de Reglamento nos presenta la figura del inversor cualificado. Para definirlo nos remite al artículo 2.e del Reglamento 2017/1129⁴⁹⁵, el cual indica que inversor cualificado son los clientes profesionales enumerados en el anexo II de MiFID II, que define como, “todo cliente que posee la experiencia, los conocimientos y la cualificación necesarios para tomar sus propias decisiones de inversión y para valorar

⁴⁹³ Artículo 3. 24 de la propuesta de Reglamento.

⁴⁹⁴ LOIS-CABALLÉ, A. (2021). “Mecanismos de protección del consumidor en la propuesta de reglamento relativo a los mercados de criptoactivos”, *Guía de criptoactivos MiCA* (Dirs. MADRID PARRA, A, PASTOR SEMPERE, M. & BLANCO SANCHEZ, M.) Ed.: Aranzadi Thomson Reuters, p. 29.

⁴⁹⁵ Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo de 14 de junio de 2017 sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE.

correctamente los riesgos inherentes a dichas decisiones”. Para ser considerado cliente profesional, el cliente debe cumplir los criterios que allí se indican ”.

MiCA centra su protección en los llamados consumidores a quienes les cobija las medidas más proteccionistas introducidas en este Reglamento. Asume que los inversores cualificados, al tener la experiencia y experticia en la materia, no requerirán de tales salvaguardias porque comprenden como evitar y enfrentar los riesgos. Esta medida, puede dejar desprotegidos en algunas situaciones a este tipo de usuarios. Huelga decir que esta tecnología crece a pasos agigantados y, puede que se dé el caso que en determinado momento un inversor cualificado no tenga los conocimientos necesarios sobre un producto en específico. En este caso, MiCA contrapone en extremos opuestos estas dos figuras como negro y blanco, sin tomar en consideración la escala de grises.

2.2 Ámbito de aplicación

MiCA somete a su regulación “a toda persona que emita criptoactivos o preste servicios relacionados con los criptoactivos en la Unión”⁴⁹⁶ y deja por fuera de su reglamentación a los criptoactivos que califiquen como instrumentos financieros⁴⁹⁷, dinero electrónico⁴⁹⁸, excepto cuando se consideren fichas de dinero electrónico en virtud del artículo 3 de MiCA; depósitos⁴⁹⁹, depósitos estructurados⁵⁰⁰ y titulizaciones⁵⁰¹. En este sentido, no se regula la tecnología Blockchain en sí misma.

2.3 ¿Qué se entiende por criptoactivo?

La propuesta de Reglamento define en el artículo 3.1.2 a los criptoactivos como “una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado o una tecnología

⁴⁹⁶ Artículo 2.1 de la propuesta de Reglamento.

⁴⁹⁷ Artículo 2.a) de la propuesta de Reglamento.

⁴⁹⁸ Artículo 2.b). La Directiva 2009/110/CE define como dinero electrónico “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, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica” distinta del emisor de dinero electrónico.

⁴⁹⁹ Artículo 2.c) de la propuesta de Reglamento.

⁵⁰⁰ Artículo 2.d) de la propuesta de Reglamento.

⁵⁰¹ Artículo 2.e) de la propuesta de Reglamento.

similar. Se puede observar que esta definición tiene un alcance amplio y no establece requisitos técnicos, sin embargo, al hacer referencia a tecnología de registros descentralizados o similar, estaría limitándose al estado de la técnica actual, por lo que, si la tecnología evoluciona de forma inesperada, puede quedar obsoleta con el paso del tiempo.

MiCA contempla varias categorías de criptoactivos, a saber, *ficha referenciada a activo* (ART, por sus siglas en inglés, *Asset-referenced tokens*), *ficha de dinero electrónico* (EMT, por sus siglas en inglés, *Electronic Money Tokens*), y *ficha de servicio* (*Utility token*). Para la regulación de ART y EMT establece un régimen regulatorio excepcional reglamentado en los títulos III y IV respectivamente, mientras que, los *Utility Token* están sujetos a la categoría general, dado que no pretende mantener ningún valor estable ni se hace referencia a moneda fiduciaria, materias primas o criptoactivos⁵⁰². Veamos de qué se trata cada uno.

3. Ficha referenciada a activo (*asset-referenced tokens* -ART).

La ficha referenciada a activo se define en MiCA como “un tipo de criptoactivo que, a fin de mantener un valor estable, se referencia al valor de varias monedas Fiat de curso legal, una o varias materias primas, uno o varios criptoactivos, o una combinación de dichos activos”⁵⁰³. Estas fichas hacen referencia a las *stablecoin* vinculadas a monedas fiduciarias, como el dólar o el euro, a materias prima como diamantes o petróleo, a criptoactivos como Bitcoin, o una combinación de todos estos activos. Un ejemplo de este token sería la criptomoneda Diem del consorcio Meta, anteriormente nombrada como Libra.

Habida cuenta de que estos tokens plantean mayores riesgos que otros criptoactivos para la protección a los consumidores,⁵⁰⁴ a los emisores se le exigen una serie de requisitos específicos en aras de garantizar su protección.

⁵⁰² ZETZSCHE, D. A., ANNUNZIATA, F., ARNER, D. W., & BUCKLEY, R. P. (2021). “The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy”. *Capital Markets Law Journal*, Vol. 16, No. 2, pp. 212-213. Disponible en: <https://academic.oup.com/cmlj/article-abstract/16/2/203/6324188?redirectedFrom=fulltext> (fecha de consulta: 22 de septiembre de 2022).

⁵⁰³ Artículo 3.1. 3) de la propuesta de reglamento.

⁵⁰⁴ Considerando 25 de la propuesta de Reglamento.

En primer lugar, para garantizar su supervisión, los emisores de estas fichas deben de tener su domicilio dentro de la UE y estar previamente autorizados por el organismo competente de su estado miembro de origen⁵⁰⁵, (donde tenga su domicilio social).

Asimismo, solo se les permitirá las ofertas públicas o la solicitud de su admisión a negociación en una plataforma de negociación de criptoactivos, si la autoridad competente ha autorizado previamente al emisor y ha aprobado el respectivo libro blanco⁵⁰⁶. Quedarán excluidos de este requisito, si durante un periodo de 12 meses el valor de las fichas no excede de cinco millones de euros o cuando la oferta esté dirigida a inversores cualificados⁵⁰⁷. Es importante destacar que los libros blancos deben estar publicados en la página web del emisor mientras estas fichas estén en manos del público⁵⁰⁸.

Los emisores de las fichas referenciadas a activos tienen la obligación de brindar información continua a los titulares de tales fichas, por lo que, como mínimo una vez al mes, deben informar en su página web la cantidad de tokens que se encuentran en circulación, la composición de sus activos de reserva (son los que estabilizan el valor de la ficha)⁵⁰⁹, o acerca de cualquier hecho que pueda afectar de forma significativa el valor de las fichas de referencias o de los activos de reserva⁵¹⁰.

Con el objetivo de estabilizar el valor de las fichas, garantizar la protección de los consumidores y prevenir el riesgo de pérdidas, es necesario que los emisores de los tokens en comento, cuenten con activos de reservas⁵¹¹ y con políticas de custodia que garanticen su separación del patrimonio del emisor. Esta medida tiene como finalidad que los activos de reserva estén libres de cargas. Es posible que una parte de los activos de reserva puedan

⁵⁰⁵ Artículo 15.1 de la propuesta de Reglamento.

⁵⁰⁶ Considerando 28 de la propuesta de Reglamento.

⁵⁰⁷ Artículo 15.3 de la propuesta de Reglamento.

⁵⁰⁸ Artículo 24 de la propuesta de Reglamento.

⁵⁰⁹ Artículo 26.1 de la propuesta de Reglamento.

⁵¹⁰ Artículo 26.3 de la propuesta de Reglamento.

⁵¹¹ Artículo 32 de la propuesta de Reglamento.

invertirse, pero está condicionado a que solo puede hacerse en instrumentos financieros que tengan una elevada liquidez y un riesgo mínimo de crédito y de mercado⁵¹².

Además, es preciso que los emisores de fichas de referencia actúen con honestidad, imparcialidad y profesionalidad⁵¹³ y se comuniquen con los titulares de dichas fichas de manera imparcial, clara y no engañosa⁵¹⁴.

Por último, se les exige a los emisores de estos tokens que cuenten con fondos propios, por un monto mínimo al importe más elevado de 350.000 euros o el 2% del importe promedio de los activos de reserva⁵¹⁵.

4. Ficha de dinero electrónico (*Electronic Money tokens* -EMT).

La ficha de dinero electrónico es definida en la propuesta de Reglamento como “un tipo de criptoactivo cuya principal finalidad es la de ser usado como medio de intercambio y que, a fin de mantener un valor estable, se referencia al valor de una moneda Fiat de curso legal”⁵¹⁶. Este token también es una *stablecoin*, pero a diferencia de los ART, para mantener estable su valor estable, emplea un único activo, que en este caso solo podría ser una moneda del curso legal. Estos criptoactivos están destinados a usarse como medio de pago⁵¹⁷ y tienen una función similar al dinero electrónico. Los emisores deben estar autorizados como entidades de crédito o de dinero electrónico⁵¹⁸, y cumplir con los requisitos de la Directiva de dinero electrónico⁵¹⁹. Asimismo, los emisores tienen la obligación de que para poder ofertar sus fichas o ser admitida a negociación en una plataforma de negociación de criptoactivos deben elaborar, publicar

⁵¹² Artículo 43 de la propuesta de Reglamento.

⁵¹³ Artículo 25.1. a) de la propuesta de Reglamento.

⁵¹⁴ Artículo 25.1. b) de la propuesta de Reglamento.

⁵¹⁵ Artículo 31.1. a). - b) de la propuesta de Reglamento.

⁵¹⁶ Artículo 3.1. 4) de la propuesta de reglamento.

⁵¹⁷ BANCO DE ESPAÑA (2022). *Informe de estabilidad...*, Op. Cit., p. 167.

⁵¹⁸ Artículo 43.1. a) de la propuesta de Reglamento.

⁵¹⁹ Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE.

y notificar a la autoridad competente⁵²⁰ un libro blanco⁵²¹(solo es notificación y no autorización, contrario a lo que sucede con los ART). Al igual que sucede con las fichas referenciadas a activos, quedan exceptuadas de los requisitos de autorización, si durante un periodo de 12 meses el umbral de los tokens no excede de cinco millones de euros o que estén destinadas a ofertarse y adquirirse por inversores cualificados⁵²².

MiCA reconoce a los titulares de EMT un crédito frente al emisor⁵²³ y el derecho a solicitar en cualquier momento el reembolso y a la par el valor monetario de la moneda fiduciaria a la que está referenciada la ficha de dinero electrónico⁵²⁴. A los emisores se les permite cobrar una comisión, solo si se indica en el libro blanco y debe ser proporcionada y adecuada con los costos reales⁵²⁵.

5. Ficha de servicio (*Utility token*).

La propuesta define a la ficha de servicio como “un tipo de criptoactivo usado para dar acceso digital a un bien o un servicio, disponible mediante TRD, y aceptado únicamente por el emisor de la ficha en cuestión”⁵²⁶. Si bien los *utility tokens* pueden captar dinero del público para financiar el desarrollo de un proyecto, su objetivo no es la de ser una inversión para sus titulares, sino de que estos tengan acceso al bien o al servicio del emisor⁵²⁷, es decir, que no son considerados como un producto financiero. Estos criptoactivos se encuentran regulados en el régimen general, su regulación es menos estricta, ya que no se consideran peligroso para los consumidores y la estabilidad financiera de la Unión Europea.

Los emisores de esta categoría no tienen que observar las obligaciones especiales que se les exige a los ART y EMT, prueba de ello es que para poder ofertar criptoactivos o solicitar su admisión a negociación en una plataforma de negociación de criptoactivos,

⁵²⁰ De acuerdo al Artículo 3.1.22.e) de la propuesta de Reglamento, la autoridad competente será el estado miembro donde ha sido autorizado como entidad de crédito o entidad de dinero electrónico.

⁵²¹ Artículo 43. 1. C) de la propuesta de Reglamento.

⁵²² Artículo 43. 2 de la propuesta de Reglamento.

⁵²³ Artículo 44.2 de la propuesta de Reglamento.

⁵²⁴ Artículo 44.3 de la propuesta de Reglamento.

⁵²⁵ Artículo 44.4 de la propuesta de Reglamento.

⁵²⁶ Artículo 3.1. 5) de la propuesta de reglamento.

⁵²⁷ PRICE WATERHOUSE COOPERS. (2021). *El impacto regulatorio ..., Op. Cit.*, p. 5.

necesitan ser persona jurídica⁵²⁸ (incluso pueden estar registrados fuera de la UE), esto significa que no deben estar autorizados por ninguna autoridad⁵²⁹. De igual forma, deben elaborar, notificar y publicar el libro blanco que debe contener la información obligatoria. Es decir, que no es necesaria la autorización de dicho documento. De igual forma se reconocen una serie de derechos a los consumidores, los cuales abordaremos en la siguiente sección.

6. Proveedores de servicios de criptoactivos

Como bien señala el informe de PWC (*Price Waterhouse Coopers*)⁵³⁰, el ámbito objetivo de la propuesta de Reglamento no solo incluye el proceso de emisión de ciertos criptoactivos, sino que además reglamenta las actuaciones de los proveedores de servicios de criptoactivos, que según MiCA es “la persona cuya actividad o negocio consiste en la prestación profesional de uno o varios servicios de criptoactivos a terceros”⁵³¹. Además, se establecen una lista cerrada de servicios y actividades que son consideradas como prestación de servicios de criptoactivos. Tales servicios son:

- i. La custodia y la administración de criptoactivos por cuenta de terceros;
- ii. La explotación de una plataforma de negociación de criptoactivos;
- iii. El canje de criptoactivos por una moneda Fiat de curso legal;
- iv. El canje de criptoactivos por otros criptoactivos;
- v. La ejecución de órdenes relacionadas con criptoactivos por cuenta de terceros;
- vi. La colocación de criptoactivos;

⁵²⁸ Artículo 4.1.a).

⁵²⁹ Quedan exceptuados de este requisito si los criptoactivos que se ofrecen son gratuitos, si durante un periodo de 12 meses el valor total de la oferta en la Unión no excede un millón de euros o la oferta esté dirigida a menos de 50 personas o a adquirirse por parte de inversores cualificados, véase Artículo 4.2 de la propuesta de Reglamento.

⁵³⁰ PRICE WATERHOUSE COOPERS. (2021). *El impacto regulatorio...*, Op. Cit., p. 18.

⁵³¹ Artículo 3.1.8) de la propuesta de Reglamento.

vii. La recepción y transmisión de órdenes relacionadas con criptoactivos por cuenta de terceros;

viii. El asesoramiento sobre criptoactivos.

Es importante destacar que, las plataformas de intercambio de criptoactivos y las billeteras entrarían en esta categoría. No obstante, esta lista ha sido objeto de críticas por parte de la doctrina, puesto que al ser una lista de *números clausus*, puede conllevar a que algunos proveedores eludan la regulación y, por tanto, sus responsabilidades⁵³². Por ejemplo, en esta lista no se encuentra el intercambio de criptoactivos por instrumentos financiero⁵³³.

Por otra parte, como medidas para garantizar la protección de los consumidores, MiCA exige que estos proveedores estén autorizados para prestar servicios de criptoactivo y tengan la condición de persona jurídica con un domicilio social en un Estado miembro de la Unión Europea⁵³⁴. Dicha autorización será válida en todo el territorio de la Unión y puede ser concedida, negada⁵³⁵ o revocada⁵³⁶ por la autoridad competente, que sería el estado miembro donde tenga su domicilio social.

Una vez se haya otorgado la autorización, la autoridad competente debe informar a la ESMA, para que esta incluya al proveedor en el Registro de proveedores de servicios de criptoactivos⁵³⁷, el cual tendrá de carácter público y estará disponible en la página web de la ESMA.

La propuesta de Reglamento impone una serie de obligaciones generales a los proveedores de servicios de criptoactivos, entre las que podemos destacar, actuación

⁵³² HORVATH, A (2021). “Protection of consumers provided in the proposal for a regulation of markets in crypto-assets”, p. 438. Disponible en: <http://pravnofakultet.rs/wp-content/uploads/2021/06/21-Agnes-Horvath.pdf> (fecha de consulta: 10 de agosto de 2022).

⁵³³ HOBZA, M., & VONDRÁČKOVÁ, A. (2021). “Crypto-asset services under the draft MiCA Regulation”, *Charles University in Prague Faculty of Law Research Paper No 2021/III/4*. Disponible en: <https://ssrn.com/abstract=3984355> (fecha de consulta 8 de agosto de 2022).

⁵³⁴ Artículo 53.1 de la propuesta de Reglamento.

⁵³⁵ Artículo 55 de la propuesta de Reglamento.

⁵³⁶ Artículo 56 de la propuesta del Reglamento.

⁵³⁷ Artículo 56.3 de la propuesta de Reglamento.

honesta, imparcial y profesional, deberán advertirles a sus clientes los riesgos asociados por la adquisición de criptoactivos, además deberán tener visible en su página web su política de precios⁵³⁸.

Asimismo, estos proveedores deberán cumplir con requisitos prudenciales en forma de fondos propios que van desde 50.000 hasta 150.000⁵³⁹, en función de la naturaleza de los servicios prestados, más una cuarta parte de los gastos fijos del año anterior⁵⁴⁰ y la adquisición de una póliza de seguro válida en toda la Unión⁵⁴¹.

De igual forma, se les exige determinados requisitos organizativos⁵⁴². Podemos destacar que, los miembros de los órganos de dirección deberán contar con la experiencia y conocimientos pertinentes para poder desempeñar sus funciones. Asimismo, tendrán la obligación de contar con un mecanismo de control interno y procedimientos de evaluación de riesgos para asegurar la seguridad, integridad y confidencialidad de la información recibida.

Por último, se establecen estrictos requisitos a los proveedores de servicios de criptoactivos que prestan servicios de custodia y administración de criptoactivos, esto es, a los famosos monederos o billeteras. Estos prestadores deberán celebrar con sus clientes contratos en donde se establezcan sus obligaciones y responsabilidades⁵⁴³. Deberán verificar la identidad de sus usuarios, lo que acaba con el seudonimato de los clientes de algunos de estos servicios. Asimismo, se les impone el deber de separar los activos de sus clientes de sus propios activos, por lo que en la Blockchain velaran para que los criptoactivos de sus clientes se encuentren en claves criptográficas (direcciones) separadas de las de sus propios criptoactivos. Asimismo, MiCA les exige contar con una política de custodia que garantice la guarda y los medios de accesos a los criptoactivos, como las claves criptográficas. (direcciones). La exigencia de esta política busca garantizar que el proveedor de servicios de criptoactivos no pueda perderlos debido a fraudes o negligencias. En este sentido, serán responsables por las pérdidas de

⁵³⁸ Artículo 59 de la propuesta de Reglamento.

⁵³⁹ Artículo 60.1. a) de la propuesta de Reglamento.

⁵⁴⁰ Artículo 60.1. b) de la propuesta de Reglamento.

⁵⁴¹ Artículo 60.4 de la propuesta de Reglamento.

⁵⁴² Artículo 61 de la propuesta de Reglamento.

⁵⁴³ Artículo 67.1 de la propuesta de Reglamento.

criptoactivos, como consecuencia de un mal funcionamiento o de pirateo informático, hasta el valor del mercado de los activos perdidos⁵⁴⁴. Aunque es importante mencionar que, la póliza de seguros contemplada en el artículo 60. 4 como parte de los requisitos prudenciales, no cubre estos casos.

Según nuestro criterio, se trata de una de las mejores medidas de MiCA, puesto que viene a corregir y poner en orden, una de las fuentes principales por las cuales la adquisición de criptoactivos es arriesgada, ya que son una de las fuentes principales de pérdidas. En este sentido, no solo se les impone barreras de entrada, que les obliga contar con unos estándares mínimos para poder operar en el mercado interno, sino que también, que en el hipotético caso de que una plataforma de intercambio de criptoactivos se declare en insolvencia o sea víctima de un ataque, será responsable ante sus clientes por las pérdidas. De modo que, no sucederá lo que hasta el momento ha venido pasando. La *Exchange* cierra y a los usuarios afectados, solo le quedan las vías judiciales para intentar recuperar los fondos custodiados por la empresa. Con MiCA los fondos de los usuarios estarán protegidos y los proveedores de servicios de criptoactivos estarán supervisados por actores institucionales.

7. Derecho de desistimiento.

El derecho de desistimiento es uno de los derechos más importantes que les otorga MiCA a los consumidores. Según la propuesta de Reglamento “Los emisores de criptoactivos, distintos de fichas referenciadas a activos y fichas de dinero electrónico, reconocerán un derecho de desistimiento a todo consumidor que compre los criptoactivos directamente al emisor o al proveedor de servicios de criptoactivos que coloque los criptoactivos por cuenta del emisor”⁵⁴⁵. Es decir, que será aplicable a los tokens que no sean fichas referenciadas a activos, ni a las fichas de dinero electrónico, por lo que, se aplicaría a las fichas de servicio.

Este derecho se puede ejercer durante los 14 días siguientes a la compra, sin que el usuario deba incurrir en gastos, o dar alguna justificación para ejercerlo⁵⁴⁶. Sin

⁵⁴⁴ Artículo 67.8 de la propuesta de Reglamento.

⁵⁴⁵ Artículo 12.1 de la propuesta de Reglamento.

⁵⁴⁶ Artículo 12.1 de la propuesta de Reglamento

embargo, tiene sus excepciones, tal y como establece el artículo 12.4 establece que no se aplicará cuando los criptoactivos hayan sido admitidos a negociación en una plataforma de negociación de criptoactivos. De tal manera, se entiende que el derecho de desistimiento no aplicaría en el caso de reventa de estos tokens, aunque se realice por parte de un profesional o a través de un mercado secundario (al no estar implicado en la transacción directamente el emisor o un proveedor de servicios de criptoactivos que coloca los criptoactivos por cuenta del emisor)⁵⁴⁷, pues en este caso, el precio dependería de las fluctuaciones de los mercados⁵⁴⁸.

Parte de la doctrina ha considerado que este derecho es insuficiente para proteger a los consumidores, ya que después de finalizado el plazo de desistimiento, estos ya no podrán retractarse y tendrán que emplear otras vías para lograrlo, posiblemente menos eficiente⁵⁴⁹.

De tal manera, en un mercado tan volátil como es el de las criptodivisas, este derecho de desistimiento parece ser inviable, sin embargo, mediante esta consideración, se logra en parte paliar el potencial especulativo de las criptodivisas.

8. Libro blanco (*whitepaper*)

La propuesta de reglamento exige a los emisores de criptoactivos, tanto para el régimen general del título II, como para las fichas referenciadas a activos y las fichas de dinero electrónico, obligaciones de información como la publicación de un libro blanco, el cual tiene una función similar al folleto informativo de las ofertas pública de venta de acciones. Para cada categoría de criptoactivos, la propuesta de reglamento impone deberes diferentes, para los emisores criptoactivos como las fichas de servicio y tokens de dinero electrónico, se exige notificación a la autoridad competente, mientras que, a los emisores de fichas referenciadas a activos, el libro blanco debe estar aprobado por la autoridad competente. Dicha aprobación es válida en toda UE. En este sentido, es importante aclarar que, a pesar de que a las fichas de dinero electrónico se les exige solo

⁵⁴⁷ PRICE WATERHOUSE COOPERS. (2021). *El impacto regulatorio...*, Op. Cit., p. 14.

⁵⁴⁸ Considerando 22 de la propuesta de reglamento.

⁵⁴⁹ HORVATH, A (2021). “Protection of consumers...”, cit., p. 446.

notificación del libro blanco, esta laxitud se da porque previamente estas entidades han debido ser autorizadas como entidades de crédito o de dinero electrónico⁵⁵⁰.

Las pymes y las empresas emergentes estarán exentas de la publicación del libro blanco, cuando la contraprestación total de la oferta de criptoactivos no supere 1 000 000 EUR en un período de doce meses y para los emisores de ART y AMT, cuando el valor total en circulación de los criptoactivos estables sea inferior a 5000.000

El propósito de este documento, es informar a los consumidores las características y peligros que comportan la adquisición de criptoactivos, con ello, MiCA pretende corregir la opacidad, información engañosa y divulgaciones inadecuadas que actualmente se observa en algunas ICOs⁵⁵¹.

Respecto al libro blanco de criptoactivos distintos a ART y EMT, este debe incluir⁵⁵² información general del emisor, descripción del proyecto, la fecha, los derechos y obligaciones asociados a los criptoactivos y las condiciones para ejercer tales derechos, la tecnología subyacente, los riesgos asociados al emisor, los criptoactivos, la oferta pública y la ejecución del proyecto, un resumen sin tecnicismo que junto con el libro blanco ofrezca información adecuada sobre los elementos esenciales de los criptoactivos.

Asimismo, deberá tener la siguiente declaración “el emisor de los criptoactivos es el único responsable del contenido del presente libro blanco de criptoactivos. Este no ha sido revisado ni aprobado por ninguna autoridad competente de ningún Estado miembro de la Unión Europea”⁵⁵³. Además, el *whitepaper* debe contener una declaración que informe que los criptoactivos pueden: perder su valor total o parcial, no ser siempre negociables y no ser líquidos.

La notificación a la autoridad competente del libro blanco se hará 20 días hábiles anteriores a la publicación del mismo⁵⁵⁴, por lo tanto, los supervisores podrán ejercer

⁵⁵⁰ PRICE WATERHOUSE COOPERS. (2021). *El impacto regulatorio...*, Op. Cit., p.17.

⁵⁵¹ ZETZSCHE, D. A., ANNUNZIATA, F., ARNER, D. W., & BUCKLEY, R. P. (2021). “The Markets in...” cit., p. 211.

⁵⁵² Artículo 5 de la propuesta de Reglamento.

⁵⁵³ Artículo 5.3 de la propuesta de Reglamento.

⁵⁵⁴ Artículo 7. 2 de la propuesta de Reglamento.

acciones de vigilancia del Artículo 82 antes de su publicación, aunque también la pueden ejercer después. Se ha criticado el hecho de que el libro blanco solo sea notificado y no aprobado, ya que las autoridades entrarían a corregir fallas de forma *ex post*, cuando los consumidores ya han sido perjudicados por la mala conducta de los emisores⁵⁵⁵.

Los emisores de criptoactivos y sus órganos de dirección son responsables civilmente ante los clientes respecto a la información contenida en el libro blanco y en el resumen (solo si la información del resumen es engañosa, inexacta o incoherente). Los consumidores pueden reclamar daños y perjuicios, no obstante, deben demostrar que el emisor ha incumplido los requisitos de información del libro blanco que ha afectado su decisión de compra⁵⁵⁶. Es decir, que, en este caso, el usuario es quien tiene la carga de la prueba, lo cual puede llegar a ser injusto, pues puede que este no cuente con los medios de prueba necesarios para hacer valer sus derechos y más aún, si tenemos en cuenta la complejidad financiera y tecnológica de la tecnología Blockchain. Creemos que los emisores están en una mejor posición para tener el *onus probandi*. Sin embargo, estas acciones no son excluyentes con las reclamaciones de responsabilidad civil de las legislaciones nacionales⁵⁵⁷. Estas responsabilidades se extienden forma casi idéntica a los emisores de fichas referenciadas a activos⁵⁵⁸ y las fichas de dinero electrónico⁵⁵⁹.

Respecto al libro blanco de criptoactivos relativo a fichas referenciadas a activos⁵⁶⁰, además de toda la información que debe contener el libro blanco de criptoactivos (distintos de ART y AMT), debe incluir, la descripción pormenorizada de: el sistema de gobernanza del emisor, los activos de reserva, las disposiciones de custodia de los activos de reserva; la política de inversión de los activos de reserva, los derechos que le asisten a los titulares, en especial el derecho directo de reembolso o crédito sobre los activos de reserva, el procedimiento de reclamaciones y un resumen del mismo sin tecnicismo. Cuando el emisor no reconozca ningún crédito o derecho directo de

⁵⁵⁵ Véase HORVATH, A (2021). “Protection of consumers...”, *cit.*, p. 443 y ZETZSCHE, D. A., ANNUNZIATA, F., ARNER, D. W., & BUCKLEY, R. P. (2021). “The Markets in...” *cit.*, p. 213.

⁵⁵⁶ Artículo 14 de la propuesta de Reglamento.

⁵⁵⁷ Artículo 14.5 de la propuesta de Reglamento.

⁵⁵⁸ Artículo 22 de la propuesta de Reglamento.

⁵⁵⁹ Artículo 47 de la propuesta de Reglamento.

⁵⁶⁰ Artículo 17 de la propuesta de Reglamento.

reembolso a todos los titulares de estas fichas, el libro blanco deberá indicar de manera clara e inequívoca esta situación.

El libro blanco de fichas de dinero electrónico⁵⁶¹ deberá contener toda la información pertinente como, descripción del emisor y del proyecto, indicación de si el libro blanco se refiere a una oferta pública de EMT y/o la admisión de dichos tokens en una plataforma de negociación de criptoactivos, los derechos y obligaciones que le asisten a los titulares, información sobre la tecnología subyacente, los riesgos asociados con la tecnología, el emisor, las fichas y con la ejecución del proyecto. También deberá contener un resumen del libro blanco sin tecnicismos y una indicación en la que se le reconozca a los consumidores el derecho de reembolso en dinero fiduciario de sus tokens en cualquier momento y a la par.

Por último, es importante mencionar que los emisores de criptoactivos pueden emitir comunicaciones publicitarias⁵⁶² que se identifiquen como tales, si se presentan de forma imparcial, clara y no engañosa, sean coherente con el contenido del libro blanco e indiquen de la existencia del mismo y la dirección de su página web. Para las fichas referenciadas a activos, MiCA establece que las comunicaciones deben indicar cuando no se reconozca ningún crédito directo o derecho directo de reembolso a todos los titulares y las comunicaciones publicitarias de las fichas de dinero electrónico indicaran el derecho de reembolso. Todas las comunicaciones deberán ser notificadas a la autoridad competente.

9. Procedimiento para la tramitación de reclamaciones

Los emisores de tokens con referencia a activos⁵⁶³, las autoridades competentes⁵⁶⁴ y los proveedores de servicios de criptoactivos⁵⁶⁵ tienen la obligación de establecer un procedimiento de tramitación de reclamaciones, no obstante, quedan excluidos de esta obligación las fichas de dinero electrónico y los criptoactivos del régimen general. Llama

⁵⁶¹ Artículo 46 de la propuesta de Reglamento.

⁵⁶² Artículos 6, 25 y 48 de la propuesta de Reglamento.

⁵⁶³ Artículo 27 de la Propuesta de Reglamento.

⁵⁶⁴ Artículo 91 de la Propuesta de Reglamento.

⁵⁶⁵ Artículo 64 de la Propuesta de Reglamento.

la atención que estos dos últimos emisores queden excluidos de la obligación de contar con un procedimiento de manejo de quejas, ya que este se trata de uno de los mecanismos principales para garantizar la protección de los consumidores, más aún, si tenemos en cuenta que los libros blancos de estos emisores no deben ser aprobados ni controlados de forma preliminar por las autoridades competentes.

Los proveedores de servicios de criptoactivos y los emisores de fichas de referencia, deberán establecer y mantener un procedimiento eficaz y transparente que permita un manejo rápido, justo y coherente de las quejas que reciban e informar a los consumidores sobre la posibilidad de presentarlas. Además, la propuesta de Reglamento determina que las reclamaciones deben ser gratuitas, los responsables deben elaborar una plantilla para la presentación de reclamaciones, contar con un registro de todas las quejas recibidas e investigar de forma oportuna e imparcial las reclamaciones recibidas.

10. Prevención del abuso del mercado

MiCA prohíbe determinadas conductas, con el objetivo de prevenir el abuso del mercado cuando los criptoactivos se admitan en una plataforma de negociación⁵⁶⁶, tales como, la comunicación ilícita de la información privilegiada⁵⁶⁷, las operaciones con información privilegiada⁵⁶⁸ y la manipulación del mercado⁵⁶⁹. Esta es una de las medidas más importante, habida cuenta que los mercados de criptoactivos son vulnerables a las prácticas de manipulación por la volatilidad de sus precios, la cual muchas veces es consecuencia de declaraciones o acciones de actores con reconocimiento público, como, por ejemplo, Elon Musk, que en 2021 tuiteó sobre los beneficios de bitcoin y los precios subieron y luego tuiteó sobre sus preocupaciones y los precios bajaron⁵⁷⁰.

⁵⁶⁶ Artículo 76 de la propuesta de Reglamento.

⁵⁶⁷ Artículo 79 de la propuesta de Reglamento.

⁵⁶⁸ Artículo 78 de la propuesta de Reglamento.

⁵⁶⁹ Artículo 80 de la propuesta de Reglamento.

⁵⁶⁹ Artículo 79 de la propuesta de Reglamento.

⁵⁷⁰ Musk también tuiteó sobre otras criptomonedas como DogeCoin y también subió su capitalización, véase BRYANOV, K. (2021). “Crypto’s fraught relationship with Elon Musk: Ambassador or liability?”. Disponible en: <https://cointelegraph.com/news/crypto-s-fraught-relationship-with-elon-musk-ambassador-or-liability> (fecha de consulta: 15 de agosto de 2022).

Respecto a la manipulación del mercado, el proyecto de Reglamento no la define, no obstante, establece una lista de actividades que pueden dar lugar a dicha conducta. De esa lista, debemos destacar la de: realizar operaciones, dar una orden o cualquier conducta que transmitan o puedan transmitir señales falsas o engañosas en cuanto a la oferta, la demanda o el precio de un criptoactivo, fijando su precio a un nivel anormal o artificial, ejemplo de esta conducta serían los esquemas *pump and dump*, que consisten en elevar artificialmente el precio de un criptoactivo con el objetivo de atraer inversores que compren, para que luego, los artífices de la manipulación vendan sus participaciones. También se considera manipulación del mercado, “aprovecharse del acceso ocasional o periódico a los medios de comunicación tradicionales o electrónicos para exponer una opinión sobre un criptoactivo después de haber tomado posiciones en dicho criptoactivo y beneficiar seguidamente de las repercusiones de la opinión expresada sobre el precio de dicho criptoactivo, sin haber comunicado simultáneamente ese conflicto de intereses al público de manera adecuada y efectiva”⁵⁷¹. En este sentido, se logra que los influencers sean más transparentes en relación con los criptoactivos que promueven. Estos “podrían abstenerse de utilizar los medios sociales o convencionales para provocar un descenso o un aumento del precio de las criptodivisas una vez que el reglamento entre en vigor”⁵⁷².

Asimismo, los proveedores de servicios de criptoactivos, deberán disponer de sistemas y procedimientos para supervisar y prevenir el abuso del mercado. En caso de sospecha de alguna conducta que pueda considerarse como tal, deberán notificarlo inmediatamente a su autoridad competente⁵⁷³.

11. Observaciones finales

Es evidente que ausencia de regulación de la tecnología Blockchain no solo ha sido un problema a largo plazo para las instituciones, sino también para los consumidores

⁵⁷¹ Artículo 80 2 c) de la propuesta de Reglamento.

⁵⁷² CENGIZ, F. (2021). “What the EU’s new MiCA regulation could mean for cryptocurrencies”, *LSE European Politics and Policy (EUROPP) blog*, p. 3. Disponible en: <https://blogs.lse.ac.uk/euoppblog/2021/07/05/what-the-eus-new-mica-regulation-could-mean-for-cryptocurrencies/> (fecha de consulta: 15 de agosto de 2022).

⁵⁷³ Artículo 61 de la propuesta de Reglamento.

de estos servicios y para los propios comerciantes, al enfrentarse a un mercado que no estaba regulado por ningún tipo de normativa y, por tanto, carente de garantías a priori⁵⁷⁴.

A nivel europeo la falta de una regulación común, permitió diversas normativas individuales por parte de los distintos Estados. Podemos encontrar ejemplos de países que desde un primer momento han tratado de regular las criptoactivos como Malta⁵⁷⁵ y Francia⁵⁷⁶ hasta a otros que, por fuera de la Unión, han optado por prohibir en gran medida esta actividad, pasando por aquellas que se inclinaron por una regulación más estricta e, incluso, aquellas que eligieron no tomar ningún tipo de medida⁵⁷⁷. Igualmente, nos enfrentamos a otro problema en torno al modo en el cual los Estados han pretendido regular esta nueva realidad, dado que, en la mayor parte de los casos, su actitud se ha limitado a colocar parches o remiendos en sus leyes, de manera que trataron de amoldar su legislación a esta nueva tecnología, que crecía inexorablemente y a pasos agigantados en torno a un marco regulatorio que mostraba a todas luces ser insuficiente, inabarcable, en ocasiones inexistente y sin una colaboración conjunta⁵⁷⁸.

Cabe destacar que, como ya vinieron advirtiendo las autoridades, en un tablero de juego tan complejo como el que puede ser el mercado de criptoactivos, el usuario debería recibir la mayor cantidad posible de información sobre con qué está negociando, dónde, cómo y con qué garantías. Sin embargo, esta información se ha visto que en múltiples ocasiones es escasa o, en el peor de los casos, errónea; quedando así el consumidor en una situación de franca vulnerabilidad.

La propuesta de Reglamento relativo a los mercados de criptoactivos viene a corregir esas fallas, proporcionando “un marco regulatorio personalizado para los criptoactivos que no están cubiertos por la legislación existente de servicios financieros de la UE y reemplaza cualquier marco nacional existente aplicable a dichos

⁵⁷⁴ FERREIRA, A., SANDNER, P. G., & DÜNSER, T. (2021). “Cryptocurrencies, DLT and crypto assets—the road to regulatory recognition in Europe”, p. 1 y ss. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891401 (fecha de consulta: 14 de septiembre de 2022).

⁵⁷⁵ Malta. Cap. 590, Virtual Financial Assets Act, noviembre de 2018.

⁵⁷⁶ Francia. LOI No. 2019-486, relative à la croissance et la transformation des entreprises, mayo de 2019.

⁵⁷⁷ FERREIRA, A. & SANDNER, P. (2021). “Eu search for regulatory answers to crypto assets and their place in the financial markets’ infrastructure”, *Computer Law & Security Review*, Vol. 43, p. 8. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0267364921001059> (fecha de consulta: 14 de septiembre de 2022).

⁵⁷⁸ FERREIRA, A., SANDNER, P. G., & DÜNSER, T. (2021). “Cryptocurrencies...”, *cit.* p. 12.

criptoactivos.”⁵⁷⁹. Además, introduce medidas importantes para alcanzar la protección del consumidor en relación con los riesgos que implican los criptoactivos, por ejemplo, los emisores y los proveedores de servicios de criptoactivos tendrán que solicitar una autorización en un estado miembro de la Unión, que será un pasaporte válido en todos los Estados miembros. Además, estos últimos, responderán ante sus clientes en caso de pérdidas, robos y pirateos. Se introducen medidas de información y transparencia, como la elaboración de un libro blanco, de cuya información engañosa se harán responsables los emisores de criptoactivos, así como el deber de contar con activos de reservas, entre otras medidas. Si bien es cierto que quedan excluidos de esta normatividad algunos desarrollos como los NFT y DeFi, la Comisión Europea, previa consulta a la ABE y la ESMA, deberá presentar un informe sobre la aplicación de MiCA 36 meses después de su entrada en vigor⁵⁸⁰, y si considera procedente incluirá una propuesta legislativa, lo que dejaría la puerta abierta a que en un futuro estos servicios queden regulados.

Sin embargo, la propuesta no ha estado exenta de críticas, ya que, por un lado, el reglamento está apoyando a aquellas instituciones ya autorizadas y asentadas en la Unión Europea, discriminando así a aquellas que operen por el momento en el exterior. Asimismo, los requisitos de calidad que impone el reglamento para operar bajo su ámbito de acción pueden ser demasiado rígidos para aquellas empresas emergentes que quieran iniciarse en esta actividad, poniéndolas en una situación de desventaja y disminuyendo así la competitividad del mercado, al crear obstáculos o barreras de entrada para los criptoproyectos⁵⁸¹. Por otro lado, lo restrictivo del reglamento, considerando que se precisa de definiciones más amplias y flexibles que no restrinjan el ámbito de aplicación de la normativa a medida que continua el desarrollo de esta tecnología⁵⁸². Además, es preocupante el hecho de que para las fichas de servicios o *utility tokens* exista un régimen de notificación y no de aprobación, habida cuenta de que si no hay una autoridad legal que certifique que efectivamente se trata de criptoactivos que no son instrumentos financieros regulados por MiFID II, es posible que surjan confusiones y conflictos⁵⁸³, ya que la línea que separa un token de servicio y un token de seguridad (instrumento

⁵⁷⁹ FERREIRA, A. & SANDNER, P. (2021). “Eu search...”, *cit.*, p. 12.

⁵⁸⁰ Artículo 122 de la propuesta de Reglamento.

⁵⁸¹ CENGİZ, F. (2021). “What the EU’s new...”, *cit.*, p. 2.

⁵⁸² FERREIRA, A. & SANDNER, P. (2021). “Eu search...”, *cit.*, p. 14.

⁵⁸³ ZETZSCHE, D. A., ANNUNZIATA, F., ARNER, D. W., & BUCKLEY, R. P. (2021). “The Markets in...” *cit.*, p. 220.

financiero) es bastante fina⁵⁸⁴. Por último, en relación con la protección a los consumidores, se ha criticado el hecho de que, las medidas de salvaguarda para proteger al usuario no quedan clara, son difusas y difícil de resumir y comprender por parte de un consumidor medio, que carece de conocimientos sobre el tema⁵⁸⁵. Asimismo, se ha criticado mucho el hecho de que se tenga que esperar a MiCA II, para poder regular algunos riesgos y desarrollos que no quedan comprendidos en la propuesta actual. No obstante, debemos recordar que esta tecnología crece a pasos agigantados y no podemos esperar que se abarque todo en un comienzo. En este sentido, nos parece que, teniendo en cuenta de que se trata de una tecnología que está en pleno desarrollo, la posición de la Comisión Europea es acertada, en el entendido, que se sabe de antemano, que es probable que tenga que hacerse un reajuste legislativo de cara al futuro. MICA, es a nuestro juicio, un paso importante para la protección de los consumidores.

Parece ser que la sensación general es que hemos llegado tarde en el intento de regulación de esta tecnología. De hecho, los hay que advierten, con acierto, que “el ecosistema Blockchain ha evolucionado rápidamente en la última década y superó a los reguladores, autoridades y legisladores”⁵⁸⁶. Estas afirmaciones podemos enmarcarlas en el contexto de las múltiples advertencias y notificaciones emitidas por los distintos organismos comunitarios a lo largo de los últimos años, los cuales contemplaron expectantes como se cernía sobre ellos un problema cada vez mayor sin tomar una actitud firme al respecto. Así, hasta que las entidades financieras y los organismos públicos no han objetivado que las criptomonedas, en concreto las criptomonedas estables, podían ser un problema para la economía, no han tomado medidas al respecto.

Los consumidores y usuarios deben contar con mecanismos de protección, independientemente si se utiliza una cadena de bloques o no. Los supervisores y reguladores no pueden seguir permitiendo las consecuencias catastróficas que ha traído en estos mercados la falta de regulación, es más, tienen el deber legal de hacerlo. La excusa no puede seguir siendo que la regulación sofoca la tecnología o que regular es muy pronto. En este punto es claro que la ley debe ser tecnológicamente neutral. El código

⁵⁸⁴ LEE, F. (2022).” MiCA white papers - What obligations will crypto firms have under the new European legislation?”. Disponible en: “<https://www.lexology.com/library/detail.aspx?g=beb201eb-21e9-48dd-ad90-071d368c3837> (fecha de consulta: 7 de agosto de 2022).

⁵⁸⁵ LOIS-CABALLÉ, A. (2021). “Mecanismos de protección del consumidor...”, *cit.*, p. 25.

⁵⁸⁶ FERREIRA, A. & SANDNER, P. (2021). “Eu search...”, *cit.*, p. 8.

no puede continuar siendo el único garante y más aún cuando este mercado ha demostrado que es injusto y está lleno fallos. Las soluciones a estos problemas solo se pueden encontrar en la ley, de hecho, la imposición de un marco regulatorio no solo beneficiaría la protección de los consumidores, sino que les garantizaría a las empresas seguridad jurídica para operar. Hacemos un llamado los legisladores europeos para que aprueban lo antes posible el Reglamento MICA. Mientras eso sucede, es importante que, para mitigar esos riesgos, los consumidores realicen verificaciones de diligencia debida sobre las inversiones que van a realizar o recabarla de consultores confiables y verificables.

CAPÍTULO CUARTO

BLOCKCHAIN Y LA RESOLUCIÓN DE DISPUTAS DESCENTRALIZADA

CAPÍTULO CUATRO: BLOCKCHAIN Y LA RESOLUCIÓN DE DISPUTAS DESCENTRALIZADA

I. JUSTICIA DESCENTRALIZADA: RESOLUCIÓN DE DISPUTAS EN BLOCKCHAIN

1. Introducción

A pesar de que muchos tecnócratas afirman que el advenimiento de la tecnología Blockchain y los contratos inteligentes garantizan de que no haya disputas, por el hecho de que las obligaciones se ejecutan de forma automática, lo cierto es que ninguna cantidad ingente de código evitará las controversias⁵⁸⁷. Inevitablemente, pueden surgir fallos en el *software* o diferencias entre las partes en el mundo físico, por lo que es muy utópico pensar que el código anulará el litigio. Como acertadamente señala NOUR- SHEHATA “esa opinión ignora la forma en que generalmente surgen las disputas en la vida real”⁵⁸⁸, pues Blockchain solo puede garantizar la ejecución en el ciberespacio, no obstante, gran parte del desempeño de los contratos tiene lugar fuera de la cadena de bloques⁵⁸⁹.

Pese a que la ejecución automática, sin intervención humana, puede dotar en términos de eficiencia al contrato, indefectiblemente surgirán controversias y, más aún, en un entorno potencialmente lucrativo, novedoso y complejo, como es, el caso de Blockchain⁵⁹⁰. Por tanto, es imprescindible que el acuerdo esté sometido dentro de un marco legal válido, para que las partes involucradas puedan solucionar sus disputas, a través de un mecanismo de resolución eficiente y vinculante.

Actualmente, el derecho internacional privado cuenta con herramientas necesarias para solucionar disputas entre partes ubicadas en diferentes Estados, sin embargo, con

⁵⁸⁷ SCHMITZ, A.J. (2020). “Resolving a New Kind of Trade War Through ODR”, p. 2. Disponible en: <https://papers.ssrn.com/abstract=3525767> (fecha de consulta: 24 de febrero de 2020).

⁵⁸⁸ SHEHATA, I. (2019). “Smart Contracts & International Arbitration”. Disponible en: <https://ssrn.com/abstract=3290026> (fecha de consulta: 21 de febrero de 2021).

⁵⁸⁹ TEVENDALE, C. & MORGAN, C. (2018). “Blockchain and smart contracts: novel opportunities for improving efficiency in contract execution and dispute resolution”. Disponible en: <https://www.herbertsmithfreehills.com/latest-thinking/blockchain-and-smart-contracts-novel-opportunities-for-improving-efficiency-in> (fecha de consulta: 10 de febrero de 2021).

⁵⁹⁰ RABINOVICH-EINY, O. & KATSH, E. (2019). “Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution”. p. 47. Disponible en: <https://papers.ssrn.com/abstract=3508461> (fecha de consulta: 24 de febrero de 2020).

Blockchain, estos mecanismos pueden verse como obsoletos o inadecuados. Características como la inmutabilidad, el anonimato y la descentralización geográfica, suponen un verdadero desafío para el sistema tradicional. Ello unido a la complejidad técnica de la tecnología, al gran volumen creciente de transacciones de bajo impacto y al hecho de que los contratos inteligentes que se ejecutan en una cadena de bloques no se pueden eliminar o editar más allá de los parámetros de su codificación⁵⁹¹. ¿Cómo se resolverán las disputas entre usuarios anónimos?, ¿cuál es la ley es aplicable?, ¿qué Tribunal es competente? En caso de superar estas limitaciones, ¿cómo puede la decisión de un juez actualizar el estado del contrato inteligente si este no se puede editar?

En resumen, estas características crean nuevas formas de disputas, que implican un gran desafío para el derecho, pues son asuntos que nunca antes han tenido que ser abordados, a pesar de que internet ya había generado tensiones, el sistema de pagos tradicional supuso un punto de estrangulamiento para el anonimato en la red. No obstante, el pago con criptomonedas cambia las reglas del juego, ya que no es fácil conocer la identidad de los contratantes.

Una cadena de bloques está expuesta a muchos tipos de controversias⁵⁹², a saber, disputas no transaccionales, que no están relacionada con las transacciones, sino con el comportamiento de las partes en el mundo real; disputas de gobernanza por fuera de Blockchain, hace referencia a los asuntos de gobernanza de la red como, por ejemplo, cuando se quiere hacer un ajuste al *software* y, por último, disputas en la cadena de bloques, las cuales tiene relación con las transacciones que deben registrarse en la Blockchain.

Blockchain requiere mecanismos de resolución de disputas que se adapten a las particularidades de esta tecnología, pero que sean eficaces, rápidos y seguros, y parece que en principio la justicia ordinaria no ofrece. Como respuesta, han surgido formas novedosas de solución de controversias. Varias *Startups* del sector Blockchain están

⁵⁹¹ GOLDENFEIN, J. & LEITER, A. (2018). "Legal engineering on the blockchain: Smart contracts as legal conduct", *Law and Critique*, Vol. 29, No. 2, p. 144. Disponible en: <https://link.springer.com/article/10.1007/s10978-018-9224-0> (fecha de consulta: 3 de febrero de 2021).

⁵⁹² Esta clasificación es presentada por el Foro económico Mundial en un informe presentado por la entidad en diciembre de 2020, véase. WORLD ECONOMIC FORUM (2020). *Bridging the Governance Gap: Dispute resolution for blockchain-based transactions- White Paper*, p. 7. Disponible en: <https://www.weforum.org/whitepapers/bridging-the-governance-gap-dispute-resolution-for-blockchain-based-transactions> (fecha de consulta: 3 de febrero de 2021).

creando plataformas de resolución de disputas en línea (*Online dispute resolution*, por sus siglas en inglés ODR)⁵⁹³ que se ajustan a este entorno novedoso.

En esta sección, nos propondremos examinar los aspectos legales y prácticos de estas nuevas plataformas de resolución de disputas, los desafíos jurídicos a los cuales se enfrentan y, la viabilidad de su adopción como mecanismos de solución de controversias para la tecnología Blockchain.

2. Resolución de Controversias en Blockchain

Existen dos métodos para resolver controversias en Blockchain, a saber, la justicia tradicional, y los mecanismos alternativos de resolución de disputas en línea, este último, para efectos prácticos de este capítulo, lo hemos dividido en dos: el arbitraje comercial internacional y los mecanismos alternativos de resolución de disputas de colaboración colectiva o *Crowdsourcing*⁵⁹⁴.

Respecto a la justicia tradicional, en caso de que los contratantes estén ubicados en diferentes estados, se aplicarían las reglas de derecho internacional, o la normatividad interna de un país, siempre y cuando los contratantes procedan de una misma jurisdicción. Esta ecuación solo funciona si conocemos la identidad de las partes, porque determina la jurisdicción competente y la ley aplicable, en caso de que estas no hayan estipulado expresamente nada en el contrato.

Sin embargo, si se desconoce la identidad y el domicilio de los contratantes, la justicia tradicional no puede establecer cuál es el Tribunal competente y la ley aplicable. Incluso, si se conociesen estos datos, su alcance sería muy limitado, “los tribunales sólo podrían obligar a las partes a ejecutar una transacción secundaria o pagar reparaciones por un contrato inteligente que generó daños para una de las partes”⁵⁹⁵ y poco más. Asimismo, no podemos dejar de lado que, dada las bases ideológicas de la tecnología, es

⁵⁹³ SCHMITZ, A.J. & RULE, C. (2019). "Online Dispute Resolution for Smart Contracts", *Legal Studies Research Paper Series*, Documento de trabajo No. 2019-11, p. 114. Disponible en: <https://papers.ssrn.com/abstract=3410450> (fecha de consulta: 5 de septiembre de 2019).

⁵⁹⁴ A lo largo de este capítulo también los llamaremos como CODR, pues los mecanismos ODR (Online dispute resolution) que utilizan crowdsourcing (colaboración abierta) han sido llamados como CODR, es decir crowdsourcing Online dispute resolution, que en español podría traducirse como resolución de conflictos en línea de colaboración abierta y distribuida.

⁵⁹⁵ KAAL, W.A. & CALCATERRA, C. (2017), "Crypto Transaction...", *cit.*, p. 41.

de esperar que los usuarios que intervengan en este tipo de contratación, vean una opción poco atractiva en la justicia tradicional, pues los jueces y tribunales son entidades centralizadas.

Los métodos de resolución de conflictos tradicionales no son muy adecuados para el entorno Blockchain, no solo por los inconvenientes que acabamos de describir, sino, además, también porque son lentos, costosos y muchas veces ineficientes. No fueron pensados para resolver disputas entre partes anónimas ubicadas alrededor del mundo, es más, puede que incluso no tengan la capacidad y la experiencia para decidir esta clase de conflictos⁵⁹⁶. Además, es muy probable, que los usuarios se apoyen más en mecanismos que sean más libertarios y estén enfocados en preservar el anonimato y la descentralización⁵⁹⁷, pues gracias a estas características es que han preferido celebrar sus acuerdos mediante contratos inteligentes y no a través de la contratación clásica. Es por esto, que el análisis de este capítulo se centrará más en métodos de resolución basados en la propia tecnología Blockchain.

3. Resolución de controversias en línea (ODR)

La resolución de disputas en línea u ODR es un “mecanismo para resolver controversias facilitado mediante el empleo de las comunicaciones electrónicas y demás tecnología de la información y las comunicaciones”.⁵⁹⁸ En tal sentido, tal y como expone ESTEBAN DE LA ROSA, ODR no es un concepto legal, sino más bien práctico. Estas siglas son empleadas para nombrar diferentes procedimientos y técnicas de resolución de controversias que usan la tecnología⁵⁹⁹. Es decir, este sistema utiliza mecanismos alternativos de resolución de disputas como la mediación, el arbitraje o la negociación, pero lo hace a través de internet. Lo que significa que, son los equivalentes en línea de los mecanismos alternativos, es decir, es como menciona MONTESINOS “una nueva

⁵⁹⁶ SCHMITZ, A.J. (2020). “Resolving a...”, *cit.*, p. 3.

⁵⁹⁷ GOLDENFEIN, J. & LEITER, A. (2018). “Legal...”. *cit.*, p. 11.

⁵⁹⁸ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2017). *Notas técnicas de la CNUDMI sobre la solución de controversias en línea*, Viena, p. 4. Disponible en: <https://uncitral.un.org/es/texts/online/dispute> (fecha de consulta: 15 de febrero de 2021).

⁵⁹⁹ ESTEBAN DE LA ROSA, F. (2011). “Principios de protección del consumidor para una iniciativa europea en el ámbito de la resolución electrónica de diferencias (ODR) de consumo transfronterizas”, *Revista General de Derecho Europeo*, No. 25, p.5. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2502355 (fecha de consulta: 21 de enero de 2023).

modalidad de ADR”⁶⁰⁰ (*Alternative Dispute Resolution*, por sus siglas en inglés). No obstante, como razonablemente señala SCHULTZ “existen otras categorías que no hacen parte de los métodos tradicionales de resolución de controversias como: tribunales en línea, jurados en línea (...). Estos procesos son parte del movimiento ODR, porque brindan sus servicios casi exclusivamente en línea y buscan la resolución de disputas”⁶⁰¹.

Los métodos alternativos en línea surgieron debido al auge y mercantilización de internet, pues la explosión del comercio electrónico supuso un aumento de las operaciones, sobre todo las de escaso valor y, con ello, consecuentemente, el incremento en el número de controversias⁶⁰². Los sistemas tradicionales de resolución de disputas resultaron ser inaccesibles y poco prácticos para una tecnología ubicua y con un gran volumen de operaciones que involucraba bajas sumas de dinero. En este sentido la resolución de disputas en línea mejoró el acceso a la justicia en el mundo digital⁶⁰³. Como consecuencia, internet proporcionó las bases para desarrollar nuevos procedimientos de reparación innovadores, accesibles⁶⁰⁴ y eficientes, aunque no sin inconvenientes. La doctrina ha mostrado su preocupación en torno a las vulnerabilidades de seguridad de las plataformas de ODR, la falta de transparencia y de confianza en estos procesos, entre otros⁶⁰⁵. Estos procesos en línea, han allanado el camino a la hora de desarrollar soluciones para el entorno Blockchain.

Hoy en día los mecanismos ODR pueden estar vinculados a Tribunales públicos, como, por ejemplo, la plataforma ODR de la Unión Europea, o pueden existir como parte integral de sitios de comercio electrónico, como es el caso del Centro de Resoluciones de

⁶⁰⁰ MONTESINOS, A. (2021). “Inteligencia Artificial y ODR”, *Justicia algorítmica y neuroderecho*, (Dirs. BARONA-VILAR, S.), Ed: Tirant lo Blanch, p. 507.

⁶⁰¹ SCHULTZ, T. (2002). *Online Dispute Resolution: an overview and selected issues*, United Nations Economic Commission for Europe, (UNECE) Forum on Online Dispute Resolution, Genova, p. 4. Disponible en: <https://ssrn.com/abstract=898821> (fecha de consulta: 3 de febrero de 2021).

⁶⁰² RABINOVICH-EINY, O. & KATSH, E. (2019). “Blockchain...”, *cit.*, p. 57.

⁶⁰³ ABEDI, F., ZELEZNIKOW, J. & BRIEN, C. (2019). “Developing regulatory standards for the concept of security in online dispute resolution systems”, *Computer Law & Security Review*, Vol. 35, No. 5. Disponible en: <http://www.sciencedirect.com/science/article/pii/S026736491830390X> (fecha de consulta: 18 de diciembre de 2020).

⁶⁰⁴ RABINOVICH-EINY, O. & KATSH, E. (2019). “Blockchain...”, *cit.*, p. 57.

⁶⁰⁵ DIMOV, D. (2017). *Crowdsourced online dispute resolution*, Leiden University Center for Law and Digital Technologies, p. 40. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003815 (fecha de consulta: 21 de marzo de 2021).

eBay⁶⁰⁶ o el Centro de Resoluciones de Airbnb. “El potencial de la tecnología para dar respuesta a las necesidades de un comercio en línea en crecimiento constante explica la aparición de plataformas informáticas dispuestas a ofrecer esos servicios”⁶⁰⁷. En este sentido, es importante destacar la labor que ejercía en este campo Modria, una plataforma ODR, bastante exitosa, fundada por COLIN RULE, que resolvía las disputas para PayPal e eBay. Se estima que en su momento logro procesar alrededor 90 millones de disputas al año⁶⁰⁸.

La adopción de ODR viene siendo impulsada por organismos internacionales para la resolución de controversias entre empresarios y consumidores/as. En la Unión Europea, en particular, la Comisión Europea ofrece una plataforma europea de resolución de litigios en línea (RLL) para garantizar la protección de los consumidores mediante el acceso a herramientas de resolución de disputas de calidad⁶⁰⁹. En este sentido, advierte en la doctrina ESTEBAN DE LA ROSA que, el legislador europeo con el objetivo de lograr la integración del mercado interno, ha producido estas vías procesales que tienen como propósito lograr una mejor efectividad de los derechos de los consumidores, especialmente las controversias de escasas cuantía⁶¹⁰.

⁶⁰⁶ KOULU, R., (2016). “Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement” *SCRIPTed*, Vol. 113, No. 1, p. 43. Disponible en: <https://script-ed.org/?p=2669> (fecha de consulta: 24 de febrero de 2020).

⁶⁰⁷ ESTEBAN DE LA ROSA, F. (2017). “Régimen de las reclamaciones de consumo transfronterizas en el nuevo Derecho europeo de resolución alternativa y en línea de litigios de consumo”, *Revista Española de Derecho Internacional*, Vol. 69, p. 111. Disponible en: http://www.revista-redi.es/wp-content/uploads/2017/07/4_estudios_esteban_de_la_rosa_regimen_reclamaciones_consumo_transfronterizas.pdf (fecha de consulta: 22 de enero de 2023).

⁶⁰⁸ ROJAS, J. (2022). “Justicia descentralizada ¿nueva tendencia?”. Disponible en: https://www.google.com/search?q=JUSTICIA+DESCENTRALIZADA+NUEVA+TENDENCIA&rlz=1C5CHFA_e_nES903ES903&oq=JUSTICIA+DESCENTRALIZADA+NUEVA+TENDENCIA&aqs=chrome..69i57j69i60.9664j0j7&sourceid=chrome&ie=UTF-8 (fecha de consulta: 18 de enero de 2023).

⁶⁰⁹ “Resolución de litigios en línea – acerca de la plataforma RLL”. Disponible en: <https://ec.europa.eu/consumers/odr/main/?event=main.home.howitworks> (fecha de consulta: 1 de marzo de 2021). Asimismo, la Unión Europea ha impulsado su uso en el artículo 17 de la Directiva de comercio electrónico: “Solución extrajudicial de litigios. 1. Los Estados miembros velarán por que, en caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario del servicio, su legislación no obstaculice la utilización de los mecanismos de solución extrajudicial, existentes con arreglo a la legislación nacional para la solución de litigios, incluso utilizando vías electrónicas adecuadas. 2. Los Estados miembros alentarán a los órganos responsables de la solución extrajudicial de litigios, en particular de litigios en materia de productos de consumo, a que actúen de modo tal que proporcionen garantías de procedimiento adecuadas a las partes afectadas. 3. Los Estados miembros incitarán a los órganos responsables de la solución extrajudicial de litigios a que informen a la Comisión de las decisiones relevantes que tomen en relación con los servicios de la sociedad de la información, y a que le transmitan todos los demás datos sobre prácticas, usos o costumbres relacionados con el comercio electrónico”.

⁶¹⁰ ESTEBAN DE LA ROSA, F. (2017). “Régimen de las reclamaciones...”, *cit.*, p. 110.

La plataforma de resolución de litigios en línea de la Unión Europea, está regulada por el Reglamento 524/2013⁶¹¹, el cual establece una serie de normas que se aplican para resolver disputas de comercio electrónico entre consumidores y empresarios. Cabe resaltar, que solo se pueden solucionar controversias que se hayan originado en línea, no pudiéndose resolver otras clases de disputas que puedan surgir mediante otros métodos de comercio a distancia. El litigio puede ser iniciado tanto por el consumidor como por el empresario.

Este Reglamento se complementa con la Directiva sobre resolución alternativa de litigios en materia de consumo⁶¹², ya que la plataforma europea no resuelve las disputas per se, sino que actúa como un centro⁶¹³ que canaliza las controversias y las remite hacia los organismos de resolución alternativas de litigios (RAL) que estén adscritos a la plataforma, tratando de resolver a través de procedimientos extrajudiciales, pero que “están homologados según normas de calidad en cuanto a equidad, eficiencia y accesibilidad”⁶¹⁴ establecidas por la Unión Europea. Por otro lado, a nivel internacional, “la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) ha intentado redactar reglas de procedimiento uniformes para la ODR, pero el trabajo se ha estancado relativamente”⁶¹⁵.

4. Resolución de disputas descentralizada y distribuida

Dada la complejidad que comporta la resolución de controversias en la cadena de bloques y los contratos inteligentes, los mecanismos alternativos de resolución de disputas en línea, se presentan como los más adecuados para abordar los problemas

⁶¹¹ Reglamento (UE) 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE.

⁶¹² Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE. Adoptada por la legislación española mediante la Ley 7/2017, de 2 de noviembre, por la que se incorpora al ordenamiento jurídico español la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo.

⁶¹³ ORTOLANI, P. (2016). “Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin”, *Oxford Journal of Legal Studies*, Vol. 36, No. 3, p. 599. Disponible en: <https://academic.oup.com/ojls/article/36/3/595/1752378> (fecha de consulta: 10 noviembre 2020). Véase “Resolución de litigios en línea- Organismos de resolución de litigios”. (Sin fecha). Disponible en: <https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.adr.show> (fecha de consulta: 13 de marzo de 2021).

⁶¹⁴ “Resolución de litigios en línea - Organismos de resolución de litigios”. Disponible en: <https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.adr.show> (fecha de consulta: 13 de marzo de 2021).

⁶¹⁵ KOULU, R., (2016). “Blockchains...”, *cit.*, p. 43.

asociados a dicha tecnología, tales como, la identificación de las partes, jurisdicción⁶¹⁶ y ley aplicable. Específicamente, si los contratantes no llegan a un acuerdo mediante un mecanismo autocompositivo, el arbitraje en línea resulta muy atractivo. La flexibilidad, confidencialidad y la posibilidad de las partes para elegir a árbitros especializados y con experiencia en un área concreta, unido a la posibilidad de ejecución casi global, en virtud de la convención de Nueva York, hace que sea más fácil su adaptación a la naturaleza desintermediada y ubicua de Blockchain. Las utilidades que suponen la adopción del arbitraje han producido que varias soluciones Blockchain hayan visto su potencial y estén ensayando la utilización de este mecanismo para resolver conflictos.

En los últimos años, hemos sido testigos del desarrollo de varios proyectos de resolución de controversias dentro del ecosistema Blockchain, los cuales cuentan con diferentes niveles de especialización y servicios⁶¹⁷. En general, estas empresas emergentes son de colaboración abierta y distribuida y aunque intentan diferenciarse entre sí⁶¹⁸, cuentan con varias características comunes tales como: un sistema de incentivos económicos para los jurados que se apoya principalmente en la teoría de juegos, la inteligencia colectiva, *Crowdsourced* (CODR) y el arbitraje.

Las plataformas de resolución de conflictos que tendremos oportunidad de analizar más adelante, algunas se sustentan en sistemas de árbitros centralizados, que se encuentran asociados a una organización externa y, otras, se apoyan en sistemas descentralizados, pues se valen de los usuarios de su comunidad, para que estos sirvan de jurados. Estos servicios tienen su utilidad cuando el contrato inteligente no es suficiente para prevenir la controversia y se necesite del juicio o cognición humana para su resolución.

Técnicamente, para que estas plataformas puedan dirimir una disputa, las partes han tenido que haber designado de antemano su servicio de resolución, e incorporar en el código de contrato inteligente la admisión de terceros que puedan suspender, modificar o

⁶¹⁶ METZGER, J. (2019). “The current landscape of blockchain-based, crowdsourced arbitration”, *Macquarie LJ*, Vol. 19, p. 88. Disponible en: https://www.mq.edu.au/_data/assets/pdf_file/0010/866287/Blockchain-Based-Crowdsourced-Arbitration.pdf (fecha de consulta: 12 de diciembre de 2020).

⁶¹⁷ JEVREMOVIC, N. (2020). “Blockchain, Smart Contracts and ADR”, p. 5. Disponible en: <https://papers.ssrn.com/abstract=3699422>. (fecha de consulta: 18 de enero de 2021).

⁶¹⁸ METZGER, J. (2019). “The current ...”, *cit.*, p. 87.

rescindir el código, puesto que, si no se ha parametrizado esta opción no se puede realizar ninguna modificación.

El principal objetivo de estas empresas emergentes es proporcionar un nuevo tipo de acceso a la justicia⁶¹⁹, necesario para un entorno con unas características que representan un desafío para la resolución de controversias, pues no solo enfrentan la dificultad de adaptarse al mundo criptográfico, sino que también es indispensable que sean una solución justa, eficiente, equitativa y vinculante. Evidentemente, cada uno de estos desarrollos conduce a cuestiones de legalidad y vinculación de sus decisiones, las cuales serán analizadas en este capítulo. A continuación, abordaremos las características comunes de las plataformas en comento.

4.1 Teoría de juegos

La teoría de juegos fue formulada por primera vez JOHN VON NEUMANN y OSKAR MORGENSTERN⁶²⁰, es ampliamente usada en matemáticas, ciencias económicas, políticas y del comportamiento. Puede definirse como “el estudio de modelos matemáticos de conflicto y cooperación entre individuos racionales e inteligentes que deben tomar una decisión. Para MYERSON la teoría de juegos proporciona técnicas matemáticas generales para analizar situaciones en las que dos o más individuos toman decisiones que influirán en el bienestar del otro”⁶²¹.

Para este concepto, un juego no se refiere a diversión o entretenimiento, sino a todo tipo de interacción social entre dos o más individuos, donde los beneficios de cada uno son afectados por las decisiones tomadas por otros. Los juegos son estructuras formalizadas de incentivos⁶²². Es decir, que el resultado no solo depende de las decisiones de una persona, sino que también es el resultado de las decisiones que otros puedan llevar a cabo. Así que las elecciones de un jugador/a afectan al resto de participantes.

⁶¹⁹ METZGER, J. (2019). “The current ...”, *cit.*, p. 83.

⁶²⁰ROSS, D. (2019). “Game Theory”, *The Stanford Encyclopedia of Philosophy*. Disponible en: <https://plato.stanford.edu/archives/win2019/entries/game-theory/> (fecha de consulta: 3 de marzo de 2021).

⁶²¹ MYERSON, R (1997). *Game theory*, Harvard university press, p. 1

⁶²² SÁENZ DE CABEZÓN, E. [Derivando]. (2018). “¿Cuál es la mejor forma de pagar la cena? la teoría de juegos”, archivo de video. Disponible en: https://www.youtube.com/watch?v=HxGvzia2PcU&ab_channel=Derivando (fecha de consulta: 12 de diciembre de 2022).

Uno de los tipos de teoría de juegos que utilizan las plataformas ODR apoyadas en Blockchain es el equilibrio de Nash, un concepto desarrollado por el premio Nobel de economía JHON NASH, ampliamente conocido por la película *A Beautiful Mind*. Esta teoría trata de “cuando dos o más individuos interactúan y cada decisión individual resulta de lo que él (o ella) espera que los otros hagan. Es decir, qué debemos esperar que suceda a partir de las interacciones entre individuos”⁶²³. Cada jugador busca maximizar su beneficio individual, considerando las estrategias de los otros jugadores. La decisión de uno afecta al resto, por lo que, una vez tomada la decisión, los jugadores no tienen ningún incentivo para modificar su estrategia, entre tanto, los otros jugadores mantengan la suya. En otras palabras, “ningún jugador se arrepiente de haber jugado la acción que ha jugado en un equilibrio de Nash”⁶²⁴.

Asimismo, los desarrollos de justicia descentralizada emplean el punto de Schelling o punto focal para resolver controversias. En teoría de juegos, el punto focal es un equilibrio de Nash, desarrollado por el economista THOMAS SCHELLING, quien calificó al punto focal como una solución natural e intuitiva que las personas tienden a usar para converger su comportamiento en ausencia de comunicación⁶²⁵, “esto es, que aun cuando las personas no se conocen y, por lo tanto, no se tienen confianza, al momento de tomar una decisión en conjunto, encontrarán un punto focal”⁶²⁶.

Uno de los ejemplos que este economista empleó para ilustrar el concepto fue: imagine dos personas que no pueden comunicarse entre sí, se les piden que deben encontrarse mañana en la ciudad de Nueva York, estas personas no han recibido ningún tipo de instrucciones sobre el lugar y la hora, pero deben procurar coordinar sus previsiones para encontrarse⁶²⁷. SCHELLING le pidió a un grupo de estudiantes que respondiesen a la pregunta y la respuesta más común fue a mediodía en la *Grand Station*. Las personas escogieron el lugar y la hora, no porque tuvieran una utilidad mayor, sino

⁶²³ MONSALVE, S. (2003). “John Nash y la teoría de juegos” *Lecturas matemáticas*, Vol. 24, no 2, p. 138. Disponible en: https://www.cienciared.com.ar/ra/usr/4/26/john_nash_y_la_teor_a_de_juegos.pdf (fecha de consulta: 12 de abril de 2021).

⁶²⁴ JACKSON, M. O. (2011). “A brief introduction to the basics of game theory”, p. 6. Disponible en: <https://ssrn.com/abstract=1968579> (fecha de consulta: 12 de abril de 2021).

⁶²⁵ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 2.

⁶²⁶ YÉPEZ, M., VELA, M. & HARO, B. (2020). “Smart contracts y el arbitraje: hacia un modelo de justicia deslocalizado”, *USFQ Law Review*, Vol. 7, No. 1, p. 16. Disponible en: <https://revistas.usfq.edu.ec/index.php/lawreview/article/view/1698> (fecha de consulta: 5 de febrero de 2021).

⁶²⁷ SCHELLING, T. (1964). *La estrategia del conflicto*, Tecnos, Madrid, p. 74.

porque es un lugar con una tradición como punto de encuentro en la ciudad de Nueva York, lo que lo convierte como un punto focal natural⁶²⁸.

De igual forma, se utiliza otro concepto de teoría de juegos no cooperativo (significa que no existe la cooperación entre los participantes), el juego de suma cero, que puede describirse como, la ganancia de un jugador, es la pérdida del otro⁶²⁹, aunque el resultado sea individual, la ganancia o la pérdida de un jugador, afecta la del otro, es decir, para que un jugador gane el otro tiene que perder⁶³⁰. En otras palabras, para que un jugador obtenga alguna rentabilidad o beneficio, se tiene que afectar al resto de participantes, porque su ganancia proviene de la pérdida del otro.

Como hemos mencionado, Varias plataformas ODR basadas en Blockchain utilizan la teoría de juegos como un método para prevenir la corrupción e incentivar económicamente a los jurados o árbitros. Explica AST que, no se espera que los agentes actúen honestamente por un código ético o por razones morales, sino porque estos hacen parte de un conjunto de reglas institucionales en las que es de interés racional actuar de esa manera para ganar⁶³¹, entre mejor lo hagan, mayor será su recompensa.

Por lo general, estos deben elegir entre dos opciones la decisión final del caso. Cada miembro del tribunal debe apostar unas fichas que, casi siempre, son el token nativo de la plataforma en la cual se está dirimiendo la disputa. Los jugadores que han apostado por la decisión tomada por la mayoría mantienen sus tokens, mientras que, los que han apostado por la decisión minoritaria los pierden y, estos son repartidos entre los usuarios ganadores. Los desarrolladores de estas plataformas argumentan que, este sistema desincentiva a que personas sin conocimientos sobre la materia de la controversia participen como jurados, porque si una persona no domina un tema, lo más probable es que su voto no lo haga de forma coherente, por lo que su decisión no estará alineada con la de la mayoría, de tal forma que, los tokens que ha apostado los perderá.

⁶²⁸ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 2.

⁶²⁹ WOODS, C. (2018). “Mind games”, *Kluwer Mediation Blog*. Disponible en: <http://mediationblog.kluwerarbitration.com/2018/04/08/mind-games/> (fecha de consulta: 12 de abril de 2021).

⁶³⁰ La community layer de Jur utiliza este sistema.

⁶³¹ AST, F., & DEFFAINS, B. (2020). “When online dispute resolution meets blockchain: The birth of decentralized justice”, *Stanford Journal of Blockchain law & policy*, Vol. 4. Disponible en: <https://stanford-jblp.pubpub.org/pub/birth-of-decentralized-justice/release/1> (fecha de consulta: 22 de marzo de 2022).

4.2 Crowdsourcing

En español podría traducirse como colaboración abierta y distribuida, proviene de la unión de las palabras *crowd* que significa multitud y *Outsourcing* que quiere decir externalizar, por lo tanto, podría definirse como una herramienta para externalizar un trabajo o una tarea. Ha sido definida por la doctrina como “el acto de una empresa que toma una función que antes realizaban los empleados y la subcontrata a una red indefinida (y generalmente grande) de personas en forma de convocatoria abierta”⁶³². Un ejemplo muy popular es Wikipedia, enciclopedia editada de manera colaborativa por una red de usuarios alrededor del mundo, o Bitcoin, la criptomoneda que dio origen a la tecnología Blockchain. Otro ejemplo que vale la pena traer a colación son las plataformas de *crowdfunding*, empleadas para la financiación de proyectos de forma colectiva. En la doctrina SÁNCHEZ RUIZ DE VALDIVIA se ha ocupado de hacer un extenso análisis al respecto⁶³³.

La resolución colectiva de disputas es la práctica de reemplazar a los jueces, árbitros o mediadores por un grupo de personas llamado la multitud⁶³⁴. Varios proyectos Blockchain han propuesto descentralizar la solución de controversias a través de la externalización del litigio a un grupo mundial de árbitros y jurados⁶³⁵. El procedimiento que ofrecen, es una combinación de los métodos no tradicionales y el *Crowdsourced*⁶³⁶, por lo que, se conoce comúnmente como CODR (*Crowdsourced Online Dispute*

⁶³² HOWE, J. (2006). “The rise of crowdsourcing”, *Wired magazine*, Vol. 14, No 6. Disponible en: <https://www.wired.com/2006/06/crowds/> (fecha de consulta: 2 de abril de 2021).

⁶³³ Véase SÁNCHEZ RUIZ DE VALDIVIA, I. (2019). “Blockchain y plataformas de financiación participativa: dos retos del mercado único digital”, *Relaciones contractuales en la economía colaborativa y en la sociedad digital*, (Dir. GARCÍA GONZÁLEZ, G., & REDINHA, M.ª R.), Ed: Dykinson, pp. 353-373, SÁNCHEZ RUIZ DE VALDIVIA, I. (2019). “La protección de los usuarios en los servicios prestados por las Plataformas de Financiación Participativa de préstamo”, *Propuestas de regulación de las Plataformas de Economía Colaborativa: perspectivas generales y sectoriales*, (Dir. ORTÍ- VALLEJO, A. & RUBIO-GIMENO, G), Ed: Thomson-Reuters Aranzadi. Cizur Menor, pp. 231-256 y SÁNCHEZ RUIZ DE VALDIVIA, I. (2018). “Plataformas de financiación participativa: una alternativa sugerente a la financiación de Pymes que facilita, también, la contratación inmobiliaria e hipotecaria transfronteriza”, *Contratación Inmobiliaria e hipotecaria transfronteriza (Análisis económico, financiero, notarial, registral, judicial, fiscal y penal)*, (Dir. SÁNCHEZ RUIZ DE VALDIVIA), Ed: Thomson Reuters Aranzadi, Cizur Menor, pp. 25-105.

⁶³⁴ GUDKOV, A. (2020). “Crowd Arbitration: Blockchain Dispute Resolution”, *Legal Issues in the Digital Age*, No. 3, p. 64. Disponible en: <https://ssrn.com/abstract=3755762> (fecha de consulta: 3 de febrero de 2021).

⁶³⁵ METZGER, J. (2019). “The current ...”, *cit.*, p. 81.

⁶³⁶ En inglés, este tipo de resolución de disputas ha recibido su propio nombre, CODR, es decir, Crowdsourced Online Dispute Resolution.

Resolution). Usualmente, para prevenir la corrupción del jurado, los miembros son anónimos y no pueden comunicarse entre sí, so pena de ser sancionados.

Al utilizar a los miembros de la plataforma como jurados para dirimir controversias, estas aplicaciones suelen resolver un gran volumen de disputas, en muy poco tiempo y con costos de litigio que pueden ser incluso cero. No obstante, en algunos casos, estos usuarios no suelen tener conocimientos jurídicos, ni especializados en la materia del litigio, porque para poder ser miembro de un jurado no se les exige cualificación especial alguna, sino que se desincentiva económicamente la participación de usuarios inexpertos, pero no hay nada que les prohíba hacerlo. De este elemento, se deriva la tercera característica común que utilizan las plataformas de gestión de conflictos basadas en Blockchain, la inteligencia colectiva.

4.3 Inteligencia colectiva

La inteligencia colectiva ha sido definida por LEVY como “una forma de inteligencia universalmente distribuida, constantemente mejorada, coordinada en tiempo real, y que da lugar a la movilización efectiva de habilidades⁶³⁷”, es decir, que un grupo de individuos toma mejores decisiones que las que podría tomar un solo miembro del mismo⁶³⁸. Un ejemplo de esta afirmación, es el comodín del público del programa televisivo ¿Quién quiere ser millonario? que conduce a respuestas correctas en el 91% de los casos⁶³⁹.

La resolución de disputas de *crowdsourcing* aprovecha el principio de la sabiduría de las multitudes⁶⁴⁰ para dirimir las controversias. Con la explosión del comercio electrónico, se popularizó la colaboración colectiva y varios proyectos CODR vinculados y no vinculados al ecosistema Blockchain han venido utilizándolo. Sin

⁶³⁷ LEVY, P. (1994). *L'intelligence collective: Pour une anthropologie du cyberspace*, Ed.: La Decouverte, Paris. (English edition: LEVY, P. (1997) *Collective Intelligence: Mankind's Emerging World in Cyberspace*, Ed.: Plenum Press, New York, como se citó en: MALONE, T & BERNSTEIN, M. (2015). “Introduction” *Handbook of Collective Intelligence*, (Dirs. MALONE, T. & BERNSTEIN, M.), MIT Press, Cambridge, p. 2.

⁶³⁸ Esta idea es la tesis central de la obra: SUROWIECKI, J. (2005). *The Wisdom of Crowds: Why the Many are Smarter than the Few and How Collective Wisdom Shapes Business, Economics, Society and Nations*, Little Brown.

⁶³⁹ LEIMEISTER, J.M. (2010). “Collective Intelligence”, *Business & Information Systems Engineering*, Vol. 2, p. 245. Disponible en: <https://link.springer.com/article/10.1007%2F978-94-007-0114-8> (fecha de consulta: 8 de abril de 2021).

⁶⁴⁰ GUDKOV, A. (2020). “Crowd Arbitration...”, *cit.*, p. 65.

embargo, la inteligencia colectiva no es un fenómeno nuevo y ha estado en el punto de mira de la ciencia y la investigación (biología, ciencias sociales, ingeniería, informática, etc.) desde hace muchos años⁶⁴¹. Desde la antigua Grecia, los ciudadanos atenienses podían participar como jurados en los juicios populares, siendo escogidos mediante el *kleroterion*, un dispositivo que elegía de aleatoriamente a los 500 miembros del jurado que resolverían una controversia.

II. PLATAFORMAS DE RESOLUCION DE CONFLICTOS DE GESTION COLABORATIVA EN BLOCKCHAIN

A continuación, analizaremos algunas de las plataformas de resolución de controversias basadas en Blockchain más populares e interesantes, para ello, hemos leído y analizado los *Whitepaper* (libro blanco) que describen el funcionamiento de estos servicios. Durante esta etapa de investigación, hemos tenido que descartar plataformas que han estado funcionando hasta hace apenas unos meses, pero que han dejado de operar sin explicación alguna, entre ellas encontramos Sagewise, Jury Online y EOS.

Como tendremos oportunidad de observar, algunas de estas empresas emergentes utilizan el arbitraje comercial internacional, siguiendo las reglas de la convención de Nueva York sobre Reconocimiento de Laudos Arbitrales o Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional. En cambio, otras utilizan mecanismos alternativos de resolución de disputas colaborativos, conocido también como CODR.

1. Mecanismos alternativos de resolución de disputas colaborativo (CODR)

1.1 Kleros

Kleros es una aplicación de arbitraje descentralizada que funciona sobre Ethereum⁶⁴², es una de las plataformas de resolución de disputas de contratos inteligentes más conocida⁶⁴³ y desarrollada⁶⁴⁴ de la actualidad. Emplea la tecnología Blockchain para

⁶⁴¹ LEIMEISTER, J.M. (2010). “Collective...”, *cit.*, p. 245.

⁶⁴² AST, F & LESAEGE, C. (2019). “White Paper”, V. 1.0. 7, p. 1. Disponible en: https://kleros.io/whitepaper_es.pdf (fecha de consulta: 16 de febrero de 2021).

⁶⁴³ GUDKOV, A. (2020). “Crowd Arbitration...”, *cit.*, p. 62.

⁶⁴⁴ METZGER, J. (2019). “The current...”, *cit.*, p. 99.

el registro de los jurados, hacer cumplir la decisión y organizar su sistema de recompensa⁶⁴⁵. Kleros posee su propio Token, el *Pinakion*⁶⁴⁶ (PNK), y lo utiliza como mecanismo de teoría de juegos para incentivar a los jurados⁶⁴⁷ y lograr que estos fallen los casos de forma adecuada⁶⁴⁸. Este enfoque se inspira en la resolución de disputas de los antiguos griegos, cuyos jurados eran ciudadanos ordinarios, quienes días antes del juicio introducían una pequeña placa de bronce llamada *Pinakion* (para identificarse) en una máquina de aleatorización (*kleroterion*) la cual elegía mediante sorteo a los jurados de los Tribunales, quienes luego eran recompensados por su trabajo⁶⁴⁹.

Kleros se basa en la sabiduría de las multitudes y se apoya en la tecnología de *crowdsourcing*, pues los jurados son los mismos usuarios de la plataforma, quienes son escogidos de forma aleatoria según la cantidad de *Pinakion* que depositen⁶⁵⁰, que es el mecanismo mediante el cual los participantes expresan su interés y disponibilidad para resolver la controversia. Esto significa que, la posibilidad de ser elegido como árbitro, es directamente proporcional a la cantidad de tokens que se depositen en garantía. Y no depende de los conocimientos técnicos o jurídicos que posean sobre la materia a resolver⁶⁵¹. Estos tokens estarán en custodia hasta tanto no se resuelva el conflicto.

Los participantes que son elegidos como miembros del jurado permanecen anónimos y no se pueden comunicar entre sí⁶⁵². Se les permite el acceso a las pruebas y evidencias para que analicen el caso concreto y así poder emitir su decisión. “Para evitar la manipulación del resultado, Kleros impide que los jurados revelen sus votos antes de que el resultado se haga público”⁶⁵³. La opción con la mayor cantidad de votos es

⁶⁴⁵ GUDKOV, A. (2020). “Crowd Arbitration...”, *cit.*, p. 62.

⁶⁴⁶ Indica AST, F., & LESAEGE, C. (2019). “White...”, *cit.*, p. 23, que, el nombre hace referencia al *Pinakion*, una placa de bronce que cada ciudadano ateniense usaba como identificación personal. El *Pinakion* fue utilizado como token para seleccionar jurados en los juicios populares atenienses.

⁶⁴⁷ METZGER, J. (2019). “The current...”, *cit.*, p. 99.

⁶⁴⁸ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 1.

⁶⁴⁹ AST, F. & LESAEGE, C. (2019). “Kleros, a protocol for a Decentralized Justice System”, p. 24. Disponible en: <https://link.medium.com/bWcrPDghdgb> (fecha de consulta: 16 de febrero de 2021). Véase también: Dispute Revolution: The Kleros Handbook of Decentralized Justice, p. 24. Disponible en: <https://ipfs.kleros.io/ipfs/QmZeV32S2VoyUnqJsRRCh75F1fP2AeomVq2Ury2fTt9V4z/Dispute-Resolution-Kleros.pdf> (fecha de consulta: 20 de diciembre de 2020).

⁶⁵⁰ SCHMITZ, A.J. & RULE, C. (2019). “Online Dispute ...”, *cit.*, p. 118.

⁶⁵¹ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 6.

⁶⁵² En caso que lo hagan son sancionados, perdiendo los tokens que depositaron en garantía para dirimir la controversia.

⁶⁵³ GUDKOV, A. (2020). “Crowd Arbitration...”, *cit.*, p. 70.

considerada la ganadora⁶⁵⁴. Los jurados que se hayan decidido por la decisión vencedora se les devolverán los tokens depositados, mientras que, los que hayan votado de forma diferente a la mayoría, perderán sus *Pinakion*, que serán distribuidos a prorrata entre los jurados ganadores⁶⁵⁵. Según Kleros, este sistema garantiza que los jurados resuelvan la controversia de manera justa y honesta, pues motiva a los miembros a votar por la decisión correcta, porque se espera que los demás miembros hagan lo mismo. Esta idea de incentivos se basa en la teoría de juegos, específicamente, el punto focal, en Kleros, el Punto Focal es la honestidad y la justicia⁶⁵⁶.

Para que la disputa se resuelva a través de Kleros, el contrato inteligente debe contener una cláusula que estipule que en caso de controversia esta se resolverá en dicha plataforma y, además, se deberá determinar cuántos jurados conformaran el Tribunal y el tipo de corte en la que se llevará a cabo el litigio. Kleros cuenta con varios tribunales⁶⁵⁷ que se subespecializan en temas específicos como, comercio electrónico, transporte y seguros, los cuales tienen sus propias reglas respecto a sus políticas, costos, número de miembros a elegir y cantidad de tokens a depositar como garantía⁶⁵⁸.

Una vez surge la inconformidad, la parte insatisfecha envía el contrato y todas sus pruebas a Kleros. Asimismo, debe cumplimentar un formulario explicando las razones de su reclamo y pagar la tarifa de arbitraje, la cual depende de la complejidad del asunto. La ejecución del contrato se suspende hasta que el jurado no tome una decisión. Una vez resuelto el caso, si una de las partes no está de acuerdo con la decisión, puede apelar, sin embargo, se requerirá el doble de jurados de la instancia anterior más uno⁶⁵⁹, lo cual evidentemente encarece los costos y desincentiva las reclamaciones.

⁶⁵⁴ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 8.

⁶⁵⁵ METZGER, J. (2019). “The current...”, *cit.*, p. 99.

⁶⁵⁶ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 11.

⁶⁵⁷ AST, F. (2017). “Kleros, a Decentralized Court System for the Internet (Abridged)” Disponible en: <https://medium.com/kleros/kleros-a-decentralized-court-system-for-the-internet-abridged-1e415c04604a> (fecha de consulta: 16 de febrero de 2021).

⁶⁵⁸ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 13.

⁶⁵⁹ AST, F. & LESAEGE, C. (2019). “White...”, *cit.*, p. 9.

1.2 Aragon Court

Aragon es una aplicación descentralizada (*dApp*) que funciona sobre Ethereum y permite crear y administrar Organizaciones Autónomas Descentralizadas (DAOs)⁶⁶⁰. Sus desarrolladores conscientes de que inexorablemente habría disputas, lanzaron la Jurisdicción descentralizada de la Red de Aragón, una plataforma ODR, que tiene como objetivo ofrecer soluciones a los conflictos que puedan surgir en DAOs⁶⁶¹. Para alcanzar este objetivo, utiliza *crowdsourcing*, inteligencia colectiva y teoría de juegos, mediante la cual se incentiva a los miembros del jurado a votar honestamente valiéndose del punto Schelling.

Señala KÄRKI⁶⁶² en el *whitepaper* al igual que Kleros, las disputas que no pueden resolverse automáticamente por el código son decididas por un Tribunal, que está compuesto por usuarios anónimos de la plataforma, quienes para poder demostrar su interés de servir como “juez” deben apostar el token nativo de la plataforma, una criptomoneda llamada *ANT* (*Aragon Network Token*). Entre más token se compre, más probabilidades se tendrá de ser escogido como juez. A diferencia de Kleros, el número de jueces no lo determinan las partes del contrato, sino que por diseño la aplicación ha estipulado que sean cinco.

EL *Whitepaper* afirma además que, el proceso de resolución inicia con la reclamación de la parte inconforme, la cual debe aportar las pruebas y pagar una fianza que se mantendrá en custodia mientras se falle el proceso y, solo, se le devolverá si se resuelve a su favor. Este sistema, según Aragón, disuade los litigios innecesarios, ya que solo los usuarios con un interés legítimo pagaran la fianza. La decisión final es la que mayor número de votos obtenga. Los miembros del jurado que hayan votado por la decisión mayoritaria recuperarán sus tokens y parte de la tarifa de la disputa, mientras que los que no son mayoría, perderán sus tokens⁶⁶³.

⁶⁶⁰ CANAL LUNATICOIN. (2019). “Aragon Network con su Cofundador Jorge Izquierdo”. Disponible en: <https://youtu.be/m3EEVrZYa2o> (fecha de consulta: 22 de febrero de 2021).

⁶⁶¹ KÄRKI. T. (2017). “Aragon Network Jurisdiction Part 1: Decentralized Court”, *Aragon Blog*. Disponible en: <https://aragon.org/blog/aragon-network-jurisdiction-part-1-decentralized-court-c8ab2a675e82> (fecha de consulta: 22 de febrero de 2021).

⁶⁶² KÄRKI. T. (2017). “Aragon Network...”, *cit.*

⁶⁶³ SCHMITZ, A.J. & RULE, C. (2019). “Online Dispute...” *cit.*, p. 120.

Si las partes no están satisfechas con la decisión del Tribunal descentralizado, pueden “apelar” el fallo, esto se hace a través del pago de una fianza mayor de la que se pagó para iniciar el proceso⁶⁶⁴. Es importante destacar, que para que el litigio sea revisado en otra ronda, la fianza la deben pagar ambas partes, en caso contrario, es decir, si la garantía solo la deposita una de las partes, el fallo finaliza y se resolverá a su favor⁶⁶⁵. En esta instancia, los jueces revisarán las reglas y materiales aportados por las partes y decidirán el conflicto.

En caso de que siga habiendo inconformidad, Aragon informa en el *whitepaper* que dispone de un Tribunal Supremo, compuesto por los nueve mejores jurados de la red, que son los jueces con las mejores calificaciones en resolución de disputas, pues Aragón, a diferencia de Kleros, posee un sistema de calificación de los jueces.

El procedimiento se lleva de forma idéntica que, en las instancias anteriores, no obstante, no habrá más apelaciones, porque la decisión será definitiva. Los miembros del jurado de la ronda anterior serán sancionados o recompensados, dependiendo de la sentencia del Tribunal Supremo, es decir, que, si el Tribunal Supremo falla de acuerdo a los jueces de la primera instancia, estos recibirán una bonificación, pero si la decisión es contraria, sus tokens serán distribuidos entre los ganadores⁶⁶⁶.

1.3 Rhubarb

Rhubarb se describe a sí misma, como un ecosistema descentralizado de personas que desarrolla, financia y promueve nuevas formas de resolución alternativas de disputas, a través de Blockchain y otras aplicaciones distribuidas⁶⁶⁷. Está co-desarrollada por una de

⁶⁶⁴ RABINOVICH-EINY, O. & KATSH, E. (2019). “Blockchain...”, *cit.*, pp. 64 y ss.

⁶⁶⁵ “Aragon Whitepaper”. (2019). Disponible en: <https://github.com/aragon/whitepaper> (fecha de consulta: 15 de febrero de 2021).

⁶⁶⁶ “Dispute lifecycle”. (Sin fecha). Disponible en: <https://documentation.aragon.org/products/aragon-court/dispute-lifecycle> (fecha de consulta: 16 de julio de 2021).

⁶⁶⁷ “About Rhubarb”. (Sin fecha). Disponible en: https://www.rhucoin.com/about_rhu.aspx (fecha de consulta: 1 de marzo de 2021).

las empresas CODR más importantes de la industria, PeopleClaim⁶⁶⁸, la cual, según cifras de la misma plataforma, ha resuelto más de 30 mil casos⁶⁶⁹.

Rhubarb, posee un token nativo, llamado *RHU*, que se emplea para recompensar a los miembros por votar para crear consenso sobre temas importantes. Los usuarios también pueden recibir el pago en Bitcoin, no obstante, si lo desean, pueden optar por no recibir⁶⁷⁰ compensación alguna. El proceso es binario y propuesto por las partes. Sin embargo, los jurados pueden proponer soluciones que no hayan sido contempladas por estas. Para hacerlo, deben depositar más de la cantidad estándar de 1 RHUCoin por sugerir una solución, pero recibirán una bonificación cinco veces mayor, si la opción que sugieren logra el consenso general.”⁶⁷¹ Al igual que Kleros y Aragon, Rhubarb se basa en el enfoque de los antiguos griegos, pues ofrece una recompensa a las personas que votan por la decisión que logra resolver la controversia, mientras que castiga con la pérdida de sus tokens, si su decisión queda por fuera del consenso en el recuento final.

En el procedimiento de resolución, llamado *Poll Verdicts*, la decisión es votada democráticamente por los usuarios que han depositado Tokens para poder participar. La parte que registra el litigio puede establecer el número máximo de jurados que pueden registrar votos y la distribución de la formación y experiencia de esos jurados⁶⁷² (pueden estar especializados en temas específicos, pero la plataforma no verifica tal conocimiento). Informa la plataforma que, si las partes lo desean, el fallo que se toma a través de la encuesta puede ser vinculante, de lo contrario, les puede ayudar en los procesos de mediación no vinculante, porque son un reflejo de la opinión del público o de grupos de expertos sobre la materia. Los usuarios que participan en la encuesta no conocen la identidad de las partes en disputa, pero ellos si deben identificarse, no obstante, Rhubarb aclara que no válida esta información. A diferencia de Kleros y Aragon, los árbitros pueden discutir y debatir las

⁶⁶⁸ Véase “PeopleClaim”. (Sin fecha). Disponible en: <https://www.peopleclaim.com/> (fecha de consulta: 27 de febrero de 2021).

⁶⁶⁹ “Our Story”. (Sin fecha). Disponible en: <https://www.rhucoin.com/our-story.aspx> (fecha de consulta: 1 de marzo de 2021)

⁶⁷⁰ “Frequently asked questions”. (Sin fecha). Disponible en: <https://www.rhucoin.com/faq.aspx> (fecha de consulta: 15 de febrero de 2021).

⁶⁷¹ METZGER, J. (2019). “The current ...”, *cit.*, p. 92.

⁶⁷² METZGER, J. (2019). “The current ...”, *cit.*, p. 91.

opciones sometidas a votación hasta la fecha de la votación final, pero no tienen conocimiento acerca de la opción que va ganando.

PLATAFORMA	MECANISMO DE RESOLUCIÓN	SELECCIÓN ALEATORIA DEL JURADO	ÁRBITROS CUALIFICADOS	ELECCIÓN DE JURADOS	DECISIÓN VINCULANTE
KLEROS	CODR- Teoría de juegos.	Si.	No.	No.	No.
ARAGON	CODR- Teoría de juegos.	Si.	No.	No.	No.
RHUBARB	CODR- Teoría de juegos.	Si.	No.	No.	No.

Tabla No. 1. Mecanismos alternativos de resolución de disputas colaborativo (CODR). Elaboración propia. Decisión vinculante hace referencia si es vinculante con la convención de Nueva York o Reglamento de Arbitraje de CNUDMI.

2. Plataformas de Arbitraje en Blockchain

En este apartado, abordaremos las plataformas de resolución de conflictos de Blockchain que pretenden que sus laudos arbitrales sean uniformes y legalmente vinculantes, ya sea porque se acogen a la Convención sobre el Reconocimiento y Ejecución de las Sentencias Arbitrales Extranjeras de 1958, o porque han adaptado la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional a reglas basadas en la tecnología Blockchain. Otras, en cambio, no ofrecen servicios de solución de controversias per se, sin embargo, externalizan la función a centros autorizados. Es importante mencionar que incluimos en este grupo el Servicio de Jur, porque si bien tiene una capa que trabaja con ODR de gestión colaborativa, posee, además, un nivel arbitral.

Es imprescindible que las partes expresen su voluntad de forma clara e inequívoca de querer someterse a un tribunal arbitral. Una de las ventajas con que cuenta este método de resolución de controversias las partes pueden nombrar los árbitros, asegurándose así, la especialidad o experiencia de estos sobre el tema a resolver, estos jurados poseen facultades para decidir sobre la práctica de pruebas, oír a las partes a los peritos y testigos, nombrar peritos (salvo pacto en contrario), entre otros. Además, el laudo arbitral es vinculante y produce efecto de cosa juzgada. La ejecución de los mismos es garantizada por la justicia ordinaria.

El arbitraje es uno de los mecanismos alternativos de resolución de disputas más populares y con mejor reputación, a nivel internacional, por ejemplo, el arbitraje de inversiones es empleado para resolver controversias entre los Estados y los inversionistas extranjeros, tales disputas son resueltas por el Centro Internacional de Arreglo de Diferencias Relativas a Inversiones (CIADI) una institución que hace parte del banco mundial. “La popularidad del arbitraje en esta variedad de contextos se deriva de su percepción como rápido, neutral, informal”⁶⁷³.

2.1 Jur

Jur es una empresa de tecnología jurídica con sede en Baar, Suiza, que ha desarrollado un ecosistema basado en Blockchain que tiene como objetivo automatizar todas las fases de un contrato inteligente, desde su creación hasta el cumplimiento, y en caso de que surjan controversias, su respectiva resolución ⁶⁷⁴. Dicho ecosistema está integrado por tres elementos distintos, a saber:

- i. Jur editor: que permite a los profesionales crear y editar plantillas de contratos legales inteligentes,
- ii. Jur Marketplace: un mercado de compra y venta de contratos inteligentes
- iii. Y, por último, el sistema de resolución de disputas, que surge como una respuesta a la ineficacia de los métodos de justicia tradicional. Este sistema incluye tres mecanismos de resolución de conflictos graduados según la complejidad y valor de los mismos⁶⁷⁵: *court layer*, *open layer* y *community layer*. Cada uno de estos Servicios requiere un Token JUR para su uso, y para recompensar a los profesionales que contribuyen al funcionamiento del mismo⁶⁷⁶.

⁶⁷³ MESHEL, T., & YAHYA, M. A. (2021). “Crypto Dispute Resolution: An Empirical Study”, *Journal of Law, Technology and Policy*, Vol. 2021, No. 2, p. 197. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3975500 (fecha de consulta: 15 de diciembre de 2021).

⁶⁷⁴ JUR. (2019). “White paper”, Vol. 2.0.2, p. 5. Disponible en: <https://jur.io/wp-content/uploads/2019/05/jur-whitepaper-v.2.0.2.pdf> (fecha de consulta: 12 de febrero de 2021).

⁶⁷⁵ JUR. (2019). “White paper...”, *cit.*, p. 27.

⁶⁷⁶ JUR. (2019). “White paper...”, *cit.*, pp. 12-13.

2.1.1 Court layer

Es el nivel judicial de plataforma, dirigida a disputas de gran complejidad y valor. Es un arbitraje comercial digitalizado que garantiza que los laudos que se emitan sean vinculantes, reconocibles y ejecutables conforme a lo establecido en la Convención de Nueva York sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras⁶⁷⁷.

Jur sostiene que su arbitraje es inteligente, debido a que combina los beneficios de la tecnología Blockchain y la digitalización, con los mecanismos tradicionales de resolución de disputas⁶⁷⁸, lo que reduce los costos y el término de resolución en un proceso completamente virtual. Para poder ofrecer servicios de arbitraje en JUR, las empresas u organizaciones que lo deseen, deben registrarse como “*Hub Admin*”, y crear un “*Arbitration Hub*”⁶⁷⁹, que se debe ajustar a los principios básicos del ecosistema⁶⁸⁰.

El “*Hub Admin*”, crea el “*Arbitration Hub*” apostando tokens Jur, que sirven como fondo de garantía, ya que aseguran que las decisiones sean de alta calidad y exentas de soborno. Las personas que deseen ser árbitro deben cumplir con los requisitos establecidos por el “*Hub Admin*” del cual pretenden ser miembro⁶⁸¹.

El reglamento interno de cada Hub debe cumplir con la convención de Nueva York sobre laudos arbitrales y con las leyes nacionales donde tengan fijado su domicilio, con el fin de garantizar la legalidad de los laudos emitidos⁶⁸². No obstante, los Hub tienen cierta libertad a la hora de elegir el reglamento y el procedimiento arbitral, ya que el objetivo de Jur es crear una red global de *Hubs* que compitan entre sí, para ofrecer la mejor calidad en beneficio del mercado legal⁶⁸³.

⁶⁷⁷ JUR. (2019). “White paper...”, *cit.*, p. 12.

⁶⁷⁸ JUR. (2019). “White paper...”, *cit.*, p. 27.

⁶⁷⁹ Es como una especie de juzgado privado.

⁶⁸⁰ JUR. (2019). “White paper...”, *cit.*, p. 28.

⁶⁸¹ JUR. (2019). “White paper...”, *cit.*, p. 28.

⁶⁸² JUR. (2019). “White paper...”, *cit.*, p. 30.

⁶⁸³ JUR. (2019). “White paper...”, *cit.*, p. 30.

Para que la controversia se dirima a través de esta plataforma, el contrato (puede ser un contrato tradicional o inteligente), debe contener una cláusula compromisoria que debe especificar la ley aplicable y el centro de arbitraje. En caso de que no elijan el tipo de ley aplicable se decidirá en equidad⁶⁸⁴.

Una vez que se presente la controversia, la parte inconforme debe enviar la solicitud al centro arbitraje y realizar el pago de una tarifa⁶⁸⁵, luego se notifica a la contraparte. La selección de los árbitros se hace de forma aleatoria entre los profesionales cuyas solicitudes han cumplido los requisitos de selección de ese *Hub*⁶⁸⁶. Los árbitros pueden aceptar o rechazar la asignación, dado que en función de la calidad del servicio que prestan, estos pueden ganar o perder dinero.

El procedimiento arbitral se ejecuta en línea y todas las etapas procesales, desde la presentación hasta la decisión final, se anotarán en Blockchain, para que haya una trazabilidad de las mismas. Antes de que se emita la decisión final, el borrador del laudo arbitral será revisado por tres pares seleccionados al azar⁶⁸⁷. Dependiendo de la calificación de estos, el borrador se convertirá en laudo arbitral si la valoración es positiva, o se reasignará la decisión a un nuevo Tribunal⁶⁸⁸, si la valoración es negativa.

Los costos de la reasignación serán pagados por el fondo de garantía de cumplimiento⁶⁸⁹. En consecuencia, los árbitros ganan o pierden tokens Jur en función de la coincidencia de su decisión con la de los pares evaluadores. Este mecanismo de incentivos se basa en la teoría de juegos. Las partes reciben el laudo arbitral con un *hash* en la cadena de bloques para que puedan comprobar su contenido⁶⁹⁰ y solicitar su ejecución según los principios de la convención de Nueva York.

⁶⁸⁴ JUR. (2019). “White paper...”, *cit.*, p. 30.

⁶⁸⁵ Se divide entre el *Hub Admin* y los árbitros del *Hub*

⁶⁸⁶ JUR. (2019). “White paper...”, *cit.*, p. 31.

⁶⁸⁷ JUR. (2019). “White paper...”, *cit.*, p. 31.

⁶⁸⁸ JUR. (2019). “White paper...”, *cit.*, p. 32

⁶⁸⁹ JUR. (2019). “White paper...”, *cit.*, p. 32

⁶⁹⁰ JUR. (2019). “White paper...”, *cit.*, p. 33

2.1.2 *Open layer*⁶⁹¹

Esta capa está dirigida para resolver conflictos de bajo valor de forma rápida⁶⁹² y eficiente, esto es, de hasta 500 dólares, o disputas de cuantías medias o altas, pero que no son complejas, como un intercambio de criptomonedas entre pares⁶⁹³. Es un sistema de ODR basado en la tecnología Blockchain que utiliza un mecanismo de incentivos inspirado en la teoría de juegos y la sabiduría de las multitudes para motivar a que los votantes emitan su decisión de forma honesta. La toma de decisión está abierta a todos los participantes de la red que deseen participar, los cuales deben manifestar su interés apostando Tokens Jur, que, al igual que sucede en Kleros y Aragon, permanecerán en garantía hasta que se emita la decisión. Los participantes perderán o ganarán sus tokens en función de si han votado favor o en contra de la decisión ganadora, por tanto, serán recompensados si su voto coincide con el de mayoría y los perderán, si su voto se encuentra en la minoría⁶⁹⁴.

2.1.3 *Comunity layer*

Esta capa es un mecanismo de resolución de conflictos en línea y descentralizado y de bajo costo, destinado a resolver disputas de valor y complejidad media, cuyos jurados requieren un cierto grado de experiencia. En este sistema solo pueden participar profesionales especializados miembros de la comunidad, quienes para poder ser parte han debido cumplimentar los requisitos de ingreso estipulados por el "*Community Creator*".

Cada *Community*, no solo establece criterios objetivos de selección de los participantes, sino que, además, crea la comunidad y establece las tarifas y reglas internas de funcionamiento, como el número de votantes permitido, con el objetivo de mantenerla

⁶⁹¹ Al momento de escribir este capítulo, Jur lanzó una versión borrador de un nuevo White paper y renombran esta capa como "*Open Justice Plataform*", la cual se encuentra en desarrollo y aun no la han lanzado. Véase "Meet the Open Justice Platform" (Sin fecha). Disponible en: <https://jur.io/products/open-justice/#:~:text=Open%20Justice%20Platform,are%20enforceable%20in%20166%20countries> (fecha de consulta: 12 de marzo de 2021).

⁶⁹² En 24 horas, el sistema incentivo con más tokens a los primeros votantes lo que garantiza que se realice en el mejor tiempo posible.

⁶⁹³ JUR. (2019). "White paper...", *cit.*, p. 37.

⁶⁹⁴ JUR. (2019). "White paper...", *cit.*, p. 38.

atractiva tanto para los jurados, así como las partes, quienes la escogerán dependiendo de la calidad de sus decisiones⁶⁹⁵.

Los litigios son decididos por los votantes de acuerdo con incentivos y mecanismos de votación, que son en gran medida los mismos que los de *Open Layer*⁶⁹⁶, sin embargo, es importante subrayar que no hay un fondo de garantía⁶⁹⁷.

2.2 Juris

Juris es uno de los proyectos más interesantes del ecosistema cripto. Se describe como un sistema de resolución disputas construido para Blockchain⁶⁹⁸. Cuenta con su propio Token, *Juris token* (JRS), que se utiliza para facilitar e incentivar el comportamiento de los jueces. La plataforma se vale de mecanismos alternativos de resolución de conflictos basados en *Juris Protocol* (protocolo de juris), de tal forma que, el conflicto puede ser resuelto de forma consensuada entre las partes implicadas (mediación), o a través de arbitraje vinculante, conforme a la Convención de Nueva York⁶⁹⁹, lo que constituirá, según Juris, un sistema globalizado y descentralizado de resolución de conflictos, pero construido sobre los estándares del debido proceso⁷⁰⁰.

Para que una disputa se resuelva a través de este servicio, el código de contrato inteligente debe incluir una cláusula compromisoria que así lo estipule⁷⁰¹. Dicha cláusula debe incluir unos parámetros mínimos recomendados por la comunidad de Juris y por la Convención de Nueva York sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras. Para que la cláusula sea efectiva, se debe depositar una pequeña cantidad de Juris Token, que serán devueltos a las partes en caso de que el contrato se ejecute sin disputa. En caso de que surja una controversia, cualquiera de los contratantes

⁶⁹⁵ JUR. (2019). “White paper...”, *cit.*, pp. 43- 44.

⁶⁹⁶ JUR. (2019). “White paper...”, *cit.*, p. 42.

⁶⁹⁷ JUR. (2019). “White paper...”, *cit.*, p. 45.

⁶⁹⁸ JURIS. (2018). “White paper”, Vol. 2.0, p. 3. Disponible en: <https://getjuris.com/publications/#whitepaper> (fecha de consulta: 20 de marzo de 2021).

⁶⁹⁹ Convención sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, véase JURIS. (2018). “White paper...”, *cit.*, p 3.

⁷⁰⁰ JURIS. (2018). “White paper...”, *cit.*, p. 14.

⁷⁰¹ JURIS. (2018). “White paper...”, *cit.*, p. 16.

puede iniciar el protocolo Juris⁷⁰². El Sistema detiene la ejecución del contrato y crea una cuenta independiente para retener los fondos. La parte insatisfecha detalla los motivos de su inconformidad y adjuntan todas las pruebas y registros asociados y se notifica a la contraparte⁷⁰³. Luego, se inicia el proceso de litigio.

El protocolo de Juris consta de 3 etapas de resolución de conflictos⁷⁰⁴ basadas en el juicio humano en todos sus niveles⁷⁰⁵, pues cuenta con el acompañamiento de juristas. Veamos.

2.2.1 *SELF Mediation*

Como su nombre lo indica, se trata de auto mediación. Es un mecanismo de resolución de conflictos autocompositivo, ya que las partes por consentimiento mutuo y pacífico alcanzan una solución. Para ello, Juris proporciona a las partes una serie de herramientas y técnicas de mediación. Las herramientas permiten que, si las partes llegan a un acuerdo, el contrato puede continuar ejecutándose tal y como está escrito, de resolverse o modificarse, si los parámetros del código lo permiten⁷⁰⁶.

2.2.2 *SNAP judgment*

O simplemente juicio *SNAP* (*Neutral Arbitrator Poll*), en español, podría definirse como Votación de Arbitraje Neutral Simple. Se alcanza esta etapa si los contratantes no lograron resolver el conflicto por su cuenta. Para acceder a este juicio, las partes pueden depositar más token Juris para incentivar la labor de los juristas. Una vez se ha activado esta opción, la plataforma facilita un proceso de discusión y votación entre todos los juristas de la plataforma. Cada jurisconsulto puede dar su opción y votar de forma anónima por la solución que le parezca más equitativa. Una vez hecha la votación, las partes recibirán los resultados y una breve opinión de los votantes⁷⁰⁷. Los contratantes

⁷⁰² JURIS. (2018). “White paper...”, *cit.*, p.16.

⁷⁰³ JURIS. (2018). “White paper...”, *cit.*, p.16.

⁷⁰⁴ METZGER, J. (2019). “The current ...”, *cit.*, p. 98.

⁷⁰⁵ JURIS. (2018). “White paper...”, *cit.*, p. 3.

⁷⁰⁶ JURIS. (2018). “White paper...”, *cit.*, p. 17.

⁷⁰⁷ JURIS. (2018). “White paper...”, *cit.*, p. 17.

pueden utilizar esta información y resolver la controversia, pero deben regresar a la primera etapa (*SELF Mediation*) para poder introducirlo en el código.

2.2.3 Binding PANEL Judgment

Si las partes aún continúan sin resolver el litigio, pueden acceder a un Acuerdo Perentorio para el litigio de expertos neutrales (*Juris Peremptory Agreement for Neutral Expert Litigation*, por sus siglas, PANEL). Para escalar el proceso, nuevamente, se tendrán que depositar *Token Juris* para pagar los honorarios de los árbitros. Juris afirma que, la sentencia es legalmente vinculante en virtud de lo estipulado en la Convención de Nueva York sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras. El Tribunal estará compuesto por tres juristas, conocidos en la plataforma como *High Jurists*, pues son los que tienen el mayor nivel de reputación y experiencia⁷⁰⁸. La elección del panel estará guiada por las normas establecidas por la ONU⁷⁰⁹. Todas las etapas del proceso, como alegatos, recopilación y revisión de las pruebas, tendrán un tiempo determinado. Una vez se toma la decisión, el presidente del panel tiene la facultad de ejecutar la decisión en el Smart Contract⁷¹⁰.

2.3 CodeLegit

CodeLegit una plataforma de auditoría técnica y de resolución de disputas que ofrece servicios de arbitraje para contratos inteligentes basados en Blockchain. Para que las partes se beneficien al máximo de su servicio, CodeLegit propone que el Smart Contract incluya en su código una “*Arbitration Library*”⁷¹¹ o biblioteca de arbitraje. Simultáneamente, las partes deben celebrar un contrato legal que incluya una cláusula de arbitraje⁷¹² que haga referencia al Reglamento de arbitraje de Blockchain, unas reglas

⁷⁰⁸ JURIS. (2018). “White paper...”, *cit.*, p. 17.

⁷⁰⁹ Convención sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras y la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional.

⁷¹⁰ JURIS. (2018). “White paper...”, *cit.*, p. 17.

⁷¹¹ CODELEGIT. (Sin fecha). “CodeLegit White Paper on Blockchain Arbitration”, p. 1. Disponible en: https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit#heading=h.r6m6m18drsxo (fecha de consulta: 22 de marzo de 2021).

⁷¹² Según Codelegit dicha cláusula debe incluir lo siguiente: “Cualquier disputa, controversia o reclamación que surja de o esté relacionada con el presente contrato, o con el incumplimiento, la terminación o la invalidez del mismo, se resolverá mediante arbitraje de acuerdo con el Reglamento de Arbitraje de Blockchain. Véase CODELEGIT. (Sin fecha). “CodeLegit White...”, *cit.*, p. 1.

basadas en la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional, pero diseñadas y adaptadas al entorno Blockchain. Es decir, el acuerdo legal contiene una cláusula compromisoria, mientras que el código de contrato inteligente incluye la *Arbitration Library*, porque a diferencia de Jur, en esta plataforma se exige la existencia de un contrato legal escrito en lenguaje natural que respalde al código y lo dote de validez jurídica.

La *Arbitration Library* implementa en el código del Smart Contract, un periodo de gracia que detiene la ejecución del contrato durante un tiempo determinado, para que las partes presenten objeciones en caso de que consideren que la otra parte ha incumplido o, porque se presenten errores de codificación. Explica Markus que, si ninguno de los contratantes se opone, el contrato finaliza su ejecución. En otras palabras, esta herramienta proporciona a las partes una especie de frenado de emergencia⁷¹³ que les permite pausar, reanudar, modificar y finalizar un contrato inteligente⁷¹⁴ en caso de conflicto.

El Smart Contract inicia el proceso arbitral enviando un mensaje a CodeLegit como Autoridad Nominadora del procedimiento arbitral. Tras la recepción de un mensaje respectivo de CodeLegit, los contratos inteligentes continúan, modifican o detienen la ejecución, según sea el caso⁷¹⁵.

Los árbitros son elegidos por las contratantes, no obstante, si no pueden llegar a un acuerdo, estos serán designados por la autoridad nominadora. A continuación, el caso se envía a los árbitros electos, junto con las pruebas y toda la información relevante⁷¹⁶. Las partes presentan sus declaraciones y en caso de que se considere necesario, se realizará una audiencia, preferiblemente virtual. Posteriormente, se decide sobre el litigio y el Smart Contract continúa, modifica o finaliza su ejecución, en función de la decisión del laudo. Como quiera que algunas legislaciones exigen que la decisión se emita por

⁷¹³ CODELEGIT. (Sin fecha). “CodeLegit White...”, *cit.*, p. 2.

⁷¹⁴ “Arbitration library”. (2017). Disponible en: <https://codelegit.com/tag/arbitration-library/> (fecha de consulta: 21 de marzo de 2021).

⁷¹⁵ CODELEGIT. (Sin fecha). “CodeLegit White...”, *cit.*, p. 2.

⁷¹⁶ MARKUS. (2017). “How Smart Contract arbitration works”. Disponible en: <https://codelegit.com/author/markus/> (fecha de consulta: 23 de marzo de 2021).

escrito, el laudo se enviará a las partes por correo electrónico y el caso se cerrará. Es importante mencionar, dicho sea de paso, que las comunicaciones se realizan mediante comunicaciones electrónicas y se aseguran con un *hash* y una marca de tiempo, que se almacenan en la Blockchain de Ethereum y Bitcoin⁷¹⁷.

2.4 Mattereum

Mattereum no es un servicio de resolución de controversias per se, sino que es una plataforma de contratos inteligentes que tiene como objetivo gestionar los derechos legales sobre la propiedad física, la propiedad intelectual y los bienes raíces, en Blockchain⁷¹⁸. Para alcanzar tal propósito, Mattereum ha planteado conectar bienes y servicios del mundo físico al mundo virtual, mediante el uso de gemelos digitales y contratos ricardianos, los cuales son exigibles legalmente. Un contrato ricardiano, como hemos mencionado en el capítulo anterior, es un tipo de Smart contract escrito en lenguaje natural, pero legible por ordenador, firmado electrónicamente y registrado en la cadena de bloques mediante la asignación de un *hash*.

A pesar de que uno de los principales propósitos de la plataforma sea prevenir las disputas con la ayuda del establecimiento de un “custodio automatizado”, que se convierta en propietario legal y registrador de los bienes a lo largo de la duración del contrato⁷¹⁹; en Mattereum, son conscientes de que, aun así, habrá disputas. Por ello, el contrato ricardiano está unido a un sistema de arbitraje centralizado y externo para la resolución de controversias⁷²⁰.

A diferencia de otras aplicaciones, la idea de Mattereum es contratar árbitros profesionales independientes a la compañía y con conocimientos técnicos. El contrato deberá incluir una cláusula que exija que las controversias sean resueltas por un árbitro seleccionado por las partes. En caso de que no haya acuerdo, será designado por

⁷¹⁷ CODELEGIT. (Sin fecha). “CodeLegit White...”, *cit.*, p. 4.

⁷¹⁸ MATTEREUM. (2020). “Working Paper”, p. 2. Disponible en: <https://mattereum.com/2020/02/03/working-paper/> (fecha de consulta: 1 de abril de 2021).

⁷¹⁹ ALLEN, D., LANE, A. & POBLET, M. (2019). “The Governance of Blockchain Dispute Resolution”, *Harvard Negotiation Law Review*, Vol. 25, p. 84. Disponible en: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/haneg25&div=5&id=&page=> (fecha de consulta: 16 de agosto de 2019). Véase también MATTEREUM. (2020). “Working...”, *cit.*, p. 2.

⁷²⁰ MATTEREUM. (2020). “Working...”, *cit.*, p. 20.

Mattereum entre un panel⁷²¹. Una vez el árbitro o el cuerpo de árbitros revisa el caso concreto, emite un laudo arbitral jurídicamente vinculante y viable técnicamente.

El servicio de arbitraje de Mattereum ha sido objeto de críticas, no solo porque propone un mecanismo de resolución de disputas centralizado a proyectos descentralizados, introduciendo nuevamente los riesgos de la centralización al ecosistema Blockchain⁷²², sino también porque el procedimiento arbitral está vagamente definido y detallado⁷²³.

2.5 OpenCourt

La plataforma de contratos inteligentes, OpenLaw, ha desarrollado un sistema de arbitraje basado en Blockchain, al que ha denominado OpenCourt. Este mecanismo se basa en la utilización de Smart Contracts de la propia plataforma (OpenLaw), el cual permite a las partes confiar en un sistema descentralizado de resolución de disputas⁷²⁴. OpenCourt explica su proyecto mediante la utilización de una herramienta integrada en la plataforma para comprar y vender productos en línea, el cual emite una factura de venta de que cumple con los requisitos legales y, se firma digitalmente a través de la cadena de bloques. Dicho contrato de venta contiene una cláusula de resolución de disputas aprobada por la asociación de arbitraje JAMS⁷²⁵, lo que garantiza la ejecución de la decisión del árbitro fuera de la Blockchain. Una vez firmado el acuerdo, los fondos depositados por el comprador se colocan en una cuenta de depósito en garantía virtual⁷²⁶. Cualquiera de las partes puede invocar el procedimiento arbitral. Una vez activado, OpenCourt transfiere los activos digitales identificados a una cuenta de depósito virtual, de tal manera, que estos quedan bloqueados hasta que se tome una decisión arbitral. Las partes presentan una declaración de los hechos y la dirección Blockchain, de quien han

⁷²¹ MATTEREUM. (2020). “Working...”, *cit.*, p. 20.

⁷²² JUR. (2019). “Whitepaper...”, *cit.*, p. 56.

⁷²³ METZGER, J. (2019). “The current ...”, *cit.*, p. 90.

⁷²⁴ OPENLAW. (2018). “OpenCourt: Legally Enforceable Blockchain-Based Arbitration”. Disponible en: <https://media.consensys.net/opencourt-legally-enforceable-blockchain-based-arbitration-3d7147dbb56f> (fecha de consulta: 1 de abril de 2021).

⁷²⁵ JAMS es un centro privado de resolución alternativa de conflictos fundado en 1979, considerado como uno de los más grandes del mundo. Según cifras publicadas en su página web al año gestiona más de 18.000 casos, véase “About us - JAMS Mediation, Arbitration and ADR Services (Sin fecha). Disponible en: <https://www.jamsadr.com/about/> (fecha de consulta: 20 de abril de 2020).

⁷²⁶ ALAG, A. & RAMPHUL, S. (Sin fecha). “Interaction between blockchain technology and arbitration”. Disponible en: <http://arbitration.mu/blockchain-arbitration/> (fecha de consulta: 5 de abril de 2021).

seleccionado como árbitro. Este, una vez nombrado, se le permite el acceso a la interfaz, para que pueda revisar los hechos y las pruebas presentadas por las partes. Finalmente, el árbitro toma la decisión y los activos mantenidos en custodia se transfieren automáticamente al ganador del caso⁷²⁷.

PLATAFORMA	MECANISMO DE RESOLUCIÓN	SELECCIÓN ALEATORIA DEL JURADO	ÁRBITROS CUALIFICADOS	ELECCIÓN DE JURADOS	DECISIÓN VINCULANTE
KLEROS	CODR- Teoría de juegos.	Si.	No.	No.	No.
ARAGON	CODR- Teoría de juegos.	Si.	No.	No.	No.
RHUBARB	CODR- Teoría de juegos.	Si.	No.	No.	No.
JUR	CODR y Teoría de juegos en los niveles Open Layer y Community Layer y arbitraje y teoría de juegos en Court Layer.	No en el nivel Binding PANEL Judgment.	Si. No obstante, en Court Layer los usuarios escogen al Hub en el cual quieren resolver su disputa, el cual puede estar compuesto por profesionales especializados en la materia del conflicto.	No.	Si, en el nivel Court Layer- Convención de Nueva York.
MATTEREUM	Arbitraje externo a la plataforma	No	No informa	Si, pero si las partes no están de acuerdo, la plataforma los elige.	El servicio de arbitraje lo realiza un centro de arbitraje.
OPENCOURT	Arbitraje externo a la plataforma	No	Si	Si	Si, el centro de arbitraje que utilizan es reconocido.

Tabla No. 2. Plataformas de Arbitraje en Blockchain. Fuente: elaboración propia.

3. Jurisdicción Distribuida

Aunque no es un servicio que se esté ejecutando, es interesante la propuesta que hacen KAAL y CALCATERRA, pues evalúan un enfoque alternativo al ejercicio legal de la jurisdicción a la que llaman jurisdicción distribuida⁷²⁸, (*distributed jurisdiction*) una plataforma de código abierto que emplea soluciones criptográficas para la resolución de disputas de contratos inteligentes. Según los autores, la infraestructura legal existente no puede abordar los desafíos legales presentados por disputas que surgen en las transacciones criptográficas, puesto que existe una imposibilidad de identificar a las partes y no hay forma de establecer la ubicación ni física, ni electrónica de la cadena de bloques, pues su ubicación, es todo el mundo. En consecuencia, no se pueden aplicar las

⁷²⁷ OPENLAW. (2018). "OpenCourt...", *cit.*

⁷²⁸ KAAL, W.A. & CALCATERRA, C. (2017), "Crypto Transaction...", *cit.*, p. 1.

nociones de jurisdicción o ley aplicable. Debido a ello, concluyen que para que exista una buena gobernanza es imprescindible la adopción de soluciones inherentes a la tecnología Blockchain en sí. Proponen que los Tribunales deben dejar la resolución de conflictos a mecanismos basado en Blockchain, puesto que las respuestas deben ser criptográficas⁷²⁹.

Señalan además que, la jurisdicción distribuida debe cumplir con dos requisitos básicos: el anonimato de los usuarios y la gobernanza basada en Blockchain que, según argumentan, su propuesta de plataforma los garantiza. De igual forma, discuten que dicha plataforma ofrece resultados más dinámicos y mejores que, por ejemplo, Aragón, pues sus decisiones nos están basadas en opciones binarias, los fallos se pueden apelar indefinidamente en el tiempo, se promueve el anonimato de las partes y los jueces, los contratantes tienen la posibilidad de contar con representación jurídica⁷³⁰ y el sistema de calificación anónima de las decisiones de los jurados garantiza la calidad de las sentencias.

III. DESAFÍOS DE LAS PLATAFORMAS DE RESOLUCIÓN DE CONFLICTOS BASADAS EN BLOCKCHAIN

Esta sección está dividida en dos apartados, primero abordaremos las preocupaciones que generan los métodos de resolución de disputas que utilizan *crowdsourcing* y teoría de juegos y, por otro lado, los servicios que pretenden que sus decisiones sean legalmente vinculantes mediante el arbitraje comercial internacional.

1. Desafíos CODR

Los proyectos de resolución de disputas que utilizan CODR, como: Kleros, Aragon, Rhubarb y la *Open Layer* de Jur, están ofreciendo respuestas novedosas y adaptadas al ecosistema Blockchain, pues resuelven el conflicto entre partes anónimas, proporcionan un sistema descentralizado, rápido y económico. Propiedades casi impensables a través de las vías tradicionales de resolución de disputas. Sin embargo, los métodos utilizados por estas plataformas conducen a muchas preocupaciones y cuestiones jurídicas, que se centran principalmente en los sistemas de selección de los jurados, la falta de conocimiento jurídico de estos y, consecuentemente, en la idoneidad de la teoría

⁷²⁹ KAAL, W.A. & CALCATERRA, C. (2017), "Crypto Transaction...", *cit.*, p. 46.

⁷³⁰ KAAL, W.A. & CALCATERRA, C. (2017), "Crypto Transaction...", *cit.*, p. 58.

de juegos para impartir justicia. Como apropiadamente señala JEVREMOVIĆ, “estas plataformas se centran más en la innovación tecnológica, pero no tienen en cuenta las particularidades legales de los procesos de resolución de disputas”⁷³¹.

1.1 Selección de los jurados

En general, la selección de los jurados se hace de manera aleatoria, lo que introduce un cierto grado de arbitrariedad en la decisión. En la mayoría de las plataformas, los miembros que deseen servir como juez de una disputa, no necesitan tener conocimientos previos o experiencia sobre el asunto a resolver, ni tampoco se les exige formación jurídica. Simplemente, aquel que desee servir como jurado, solo debe demostrar su interés comprando tokens y apostar en la disputa que desee dirimir. Aunque la necesidad de tener que apostar tokens para poder participar como árbitro y la teoría de juegos desalientan la participación de usuarios inexpertos, no es suficiente para ofrecer la seguridad y garantía que brindan los jueces con experiencia. Por ejemplo, KAAL y CALCATERRA explican que la confianza de las partes en la resolución de conflictos efectiva y justa se ve socavada, lo que conduce a una menor confianza general en las transacciones criptográficas en su conjunto⁷³². Desde luego, es muy probable que los usuarios que tengan que dirimir disputas complejas y de alto valor no deseen este nivel de arbitrariedad, lo que puede menguar la adopción de Blockchain o en el mejor de los casos, queden solo relegados a asuntos más pequeños.

1.2 Justicia

El procedimiento para resolver el asunto en discusión y por el cual los jurados alcanzan el consenso es la teoría de juegos, de tal manera que, la decisión no se toma basándose en los méritos de la posición de cada parte, sino en una predicción⁷³³ de cómo creen los jurados que votarán los otros miembros, en ausencia de comunicación entre ellos⁷³⁴. Esto significa que estos procesos no suelen ser exhaustivos, ni deliberativos. A

⁷³¹ JEVREMOVIC, N. (2020). “Blockchain, Smart...”, *cit.*, p. 9.

⁷³² KAAL, W.A. & CALCATERRA, C. (2017), “Crypto Transaction...”, *cit.*, p. 52

⁷³³ WORLD ECONOMIC FORUM (2020). *Bridging the Governance ...*, *Op. cit.*, p. 13.

⁷³⁴ TSE, G. (2019). “Blockchain dispute resolution: a better alternative for the decentralised world?”. Disponible en: <https://www.taylorvinters.com/article/blockchain-dispute-resolution-a-better-alternative-for-the-decentralised-world> (fecha de consulta: 6 de febrero de 2021).

excepción de Rhubarb, los miembros del jurado no pueden discutir la decisión final., no se celebran audiencias y no se exige los jurados que razonen sus decisiones⁷³⁵. Tampoco les pueden ordenar a las partes que aporten pruebas adicionales, ni se pueden rebatir los argumentos de la contraparte. Por lo tanto, la sentencia es el resultado de una toma de decisión arbitraria, ya que los responsables de la toma de decisiones casi no tienen un marco analítico del que basarse⁷³⁶.

Ello conduce a cuestionar si en realidad la teoría de juegos es suficiente para impartir justicia, habida cuenta de que los miembros del tribunal votan guiados por sus propios intereses económicos (si su decisión no está alineada con la de mayoría, perderán los tokens depositados, por lo que su intención es conservarlos) y no en lo más justo o legalmente correcto. En este sentido, observan NAVA- GONZÁLEZ y otros que, si bien los árbitros pueden decidir en equidad, también pueden hacerlo “al azar o incluso de mala fe, en virtud de que no hay mecanismos de control, en este sentido, únicamente el estímulo de votar como la mayoría a fin ganar dinero y no perderlo”⁷³⁷.

Según los desarrolladores de estos proyectos, estos incentivos son suficientes para emitir un voto razonable, correcto, libre e independiente. Asimismo, generalmente los árbitros deben decidir su respuesta sobre dos opciones predeterminadas, decisión A o decisión B, son soluciones binarias que excluyen medidas más matizadas o flexibles que permitan a las partes no solo ganar o perder la disputa, sino un término medio. Puede que se dé el caso, que ambas partes tengan “la razón” y se busque un fallo más equitativo.

La sabiduría de los grupos no equivale a emitir un voto por el resultado legal correcto⁷³⁸ o más equitativo. Si bien es cierto que, la inteligencia colectiva logró crear

⁷³⁵ KADIOGLU KUMTEPE, C. (2020). “A Brief Introduction to Blockchain Dispute Resolution”, *John Marshall Law Journal*, Vol. 14, No. 2, p. 147. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083107 (fecha de consulta: 15 de junio de 2022).

⁷³⁶ BUCHWALD, M. (2019). “Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration”, *University of Pennsylvania Law Review*, Vol. 168, p. 1391. Disponible en: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn_law_review (fecha de consulta: 30 de enero de 2021).

⁷³⁷ NAVA- GONZÁLEZ, W. & GONZÁLEZ-MARTÍN, N. (2022). “Panorama actual de los criptotribunales arbitrales: obstáculos y consideraciones jurídicas”, *Anales de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata*, No. 52, p. 602. Disponible en: <https://revistas.unlp.edu.ar/RevistaAnalesJursoc/article/view/13518> (fecha de consulta: 16 de enero de 2023).

⁷³⁸ BUCHWALD, M. (2019). “Smart Contract...”, *cit.*, p. 1404. Véase también JEVREMOVIC, N. (2020). “Blockchain, Smart...”, *cit.*, p. 19.

una enciclopedia como Wikipedia, un sistema operativo sofisticado como Linux y una criptomoneda descentralizada como Bitcoin⁷³⁹, no todas las multitudes son eficientes⁷⁴⁰. Puede ser que, tal como advierte METZGER, jurados de diferentes jurisdicciones y culturas entiendan de forma distinta lo que se considera legal⁷⁴¹ o que tengan diferentes enfoques de equidad, ya que proceden de diferentes religiones, tradiciones y creencias⁷⁴².

En ocasiones, las masas pueden llegar a ser irracionales y tomar decisiones erróneas, como, por ejemplo, las burbujas inmobiliarias⁷⁴³. También, se puede dar el caso en que los jurados tengan sesgos cognitivos, lo que conlleva a que el punto focal en el cual convergen sea incorrecto, como, por ejemplo, lo que sucede en la película 12 hombres sin piedad, cinta dirigida por SIDNEY LUMET, narra la historia de un jurado popular compuesto por doce hombres que deben juzgar a un adolescente afroamericano, acusado de haber matado a su padre⁷⁴⁴. Si el sospechoso es hallado culpable, su pena sería la muerte. Inicialmente, la mayoría de los miembros del jurado (once) consideraron que el acusado era culpable, por una falta de análisis de las pruebas y porque tenían prejuicios por su origen racial. Sin embargo, uno de los miembros no está convencido de la culpabilidad del adolescente y logra persuadir al resto mediante el aporte de nuevas pruebas y un examen más riguroso de la evidencia. Finalmente, se logra comprobar la inocencia del acusado, por lo que se libra de ir a la silla eléctrica erróneamente. Desde luego, se trata de una ficción, pero lo realmente importante es que tal y como argumenta SUROWIECKI, un solo discrepante hace más inteligente al grupo⁷⁴⁵. Por lo tanto, las deliberaciones son necesarias, aunque ello implique que el término para resolver la disputa se extienda, de lo contrario se podrían producir decisiones menos justas⁷⁴⁶. En

⁷³⁹ AST, F., & DEFFAINS, B. (2020). "When online...", *cit.*

⁷⁴⁰ GUDKOV, A. (2020). "Crowd Arbitration...", *cit.*, p. 65.

⁷⁴¹ METZGER, J. (2019). "The current ...", *cit.*, p. 100.

⁷⁴² GUDKOV, A. (2020). "Crowd Arbitration...", *cit.*, p. 68.

⁷⁴³ SUROWIECKI, J. (2005). *Cien mejor que uno: la sabiduría de la multitud o por qué la mayoría siempre es más inteligente que la minoría*, Tendencias, p. 128.

⁷⁴⁴ LUMET, S. (1957). "Doce hombres sin piedad", *Metro-Goldwyn-Mayer*. Disponible en: <https://www.filmaffinity.com/es/film695552.html> (fecha de consulta: 23 de marzo de 2021).

⁷⁴⁵ SUROWIECKI, J. (2005). *Cien mejor...*, *Op. Cit.*, p. 100

⁷⁴⁶ GUDKOV, A. (2020). "Crowd Arbitration...", *cit.*, p. 70.

este sentido, la idea de justicia de estas plataformas, determinada por la decisión de las mayorías no tiene nada que ver con su concepción tradicional⁷⁴⁷.

1.3 Ejecución, vinculación y legalidad

No está claro cómo se pueden ejecutar el cumplimiento de las decisiones tomadas en medio de las plataformas Blockchain, porque si bien para temas que dependan del código, como transferencia de tokens o monedas, se puede programar la función en el código, hay casos que ocurren fuera de la cadena de bloques, como la entrega de un servicio o de un producto.

Estos asuntos generan problemas, porque en la mayoría de los casos, los fallos que se dictaminan en estas plataformas no tienen ningún tipo de validez legal, pues sus procedimientos no están amparados en la ley. Es más, si se diera el caso que un acuerdo de transacción celebrado con observancia de los requisitos legales, el cumplimiento no se puede forzar porque las partes no se pueden identificar.

Sin embargo, esta problemática no es exclusiva de los mecanismos alternativos de resolución de conflictos basados en Blockchain, sino de ODR en general. Para solucionar esta problemática se han ideado mecanismos de ejecución privados⁷⁴⁸ como, por ejemplo, sistemas de puntuación, sellos de confianza, depósito en garantía⁷⁴⁹ o calificación por parte de los usuarios. Estos mecanismos pueden tomarse prestado y adoptarlos en el entorno Blockchain para la ejecución de fallos que se resuelvan en dichas plataformas. Son muchas las posibilidades de ejecución privada que se pueden implementar en Blockchain, toda vez que los jurados pueden retroalimentar el código como oráculos, no obstante, esto solo puede tener lugar dentro de la cadena de bloques.

Otro de los puntos que genera preocupación en torno a estos servicios se refiere al hecho de que las disputas se resuelvan sin observancia de leyes nacionales o

⁷⁴⁷ BECKER, K. (2022). “Blockchain Matters—Lex Cryptographia ...”, *cit.*, p. 125.

⁷⁴⁸ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2013). *Solución de controversias por vía informática en las operaciones transfronterizas de comercio electrónico: visión general de los mecanismos privados de ejecución*, Viena. Disponible en: <https://undocs.org/A/CN.9/WG.III/WP.124> (fecha de consulta: 30 de enero de 2021), p. 3.

⁷⁴⁹ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2013). *Solución de controversias...*, *cit.*, p. 5.

internacionales y, priva a las partes de principios legales como el debido proceso. Como tuvimos oportunidad de ver, estas plataformas no siguen reglas sustantivas, ni procesales de legislación alguna. Incluso, jurados de proyectos como Kleros creen que no se debería determinar una jurisdicción nacional con la que la disputa esté estrechamente relacionada⁷⁵⁰. Sin duda, estos procesos rápidos y prácticos pueden llegar a ser eficientes en disputas de muy bajo valor, pero no en casos más complejos.

2. Desafíos del Arbitraje

En esta sección abordaremos las preocupaciones en torno a la adopción del arbitraje legalmente vinculante que se desarrolla en las plataformas basadas en Blockchain. Servicios como Jur (*Court Layer*), Juris (*Binding PANEL Judgment*), Codelegit y Mattereum, señalan que sus laudos siguen las reglas de la Convención de Nueva York sobre ejecución de laudos extranjeros o la Ley Modelo de la CNUDMI sobre Arbitraje Comercial, con lo cual aseguran su legalidad y ejecución.

El arbitraje internacional es un método de resolución de controversias útil para el entorno distribuido, es neutral y vinculante⁷⁵¹. Las reglas de CNUDMI son tecnológicamente agnósticas en su aplicación del comercio electrónico, por lo que pueden emplearse en la cadena de bloques para resolver controversias⁷⁵².

Asimismo, el arbitraje es flexible y se puede ejecutar fuera de Blockchain en 172⁷⁵³ países, en virtud de la Convención de Nueva York, siempre y cuando el procedimiento se ciña a lo establecido en dicha convención. Además, las partes pueden asegurar la contratación de un Tribunal que esté compuesto por árbitros especializados que comprendan las complejidades técnicas relacionadas con la tecnología⁷⁵⁴. Los

⁷⁵⁰ GUDKOV, A. (2020). “Crowd Arbitration...”, *cit.*, p. 73.

⁷⁵¹ KREIS, F. & KAULARTZ, M. (2019). “Smart Contracts and Dispute Resolution—A Chance to Raise Efficiency?”, *ASA Bulletin*, Vol. 37, No. 2, p. 342. Disponible en: <https://kluwerlawonline.com/journalarticle/ASA+Bulletin/37.2/ASAB2019031> (fecha de consulta: 17 de febrero de 2021).

⁷⁵² EVANS, T. M. (2019). “Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes”, *Wayne L. Rev.*, Vol. 65, pp. 9-10. Disponible en: https://scholars.unh.edu/cgi/viewcontent.cgi?article=1432&context=law_facpub (fecha de consulta: 16 de febrero de 2021).

⁷⁵³ Actualizado a enero de 2023.

⁷⁵⁴ ALAG, A. & RAMPHUL, S. (Sin fecha). “Interaction between...”, *cit.*

contratantes tienen la posibilidad de elegir la ley aplicable a su controversia, que, en este caso, pueden ser las más amigables con la tecnología Blockchain, como del Estado de Delaware, Tennessee o Arizona, que han aprobado leyes para reconocer los efectos legales de los contratos inteligentes⁷⁵⁵.

No obstante, existen preocupaciones en el desarrollo del arbitraje en el contexto Blockchain. Por un lado, están las cuestiones que tienen que ver con el reconocimiento y ejecución del laudo y, por otro lado, están los costos.

2.1 Reconocimiento y ejecución

Señala el artículo 2.2 de la convención de Nueva York⁷⁵⁶ que, la cláusula compromisoria debe estar por escrito, por lo tanto, esto genera inseguridad jurídica si la cláusula está contenida solo en el código. Sin embargo, la enmienda de ley modelo de arbitraje aprobada en 2006⁷⁵⁷ aclara que un acuerdo ha sido por escrito, si se ha comunicado de forma electrónica, lo que deja la puerta abierta a que se le reconozca validez jurídica a un acuerdo escrito en lenguaje de programación, si lo interpretamos de forma amplia. Asimismo, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (ningún Estado de la Unión Europea es parte) adopta el principio de la equivalencia funcional entre comunicaciones electrónicas y los documentos en papel⁷⁵⁸. Específicamente, se establecen los criterios mínimos en los cuales determinados conceptos tradicionales como, por ejemplo, escrito, firma, original y registro se puedan satisfacer mediante comunicaciones electrónicas⁷⁵⁹. Consideramos que la cláusula arbitral codificada en el Smart Contracts eventualmente podría considerarse válida conforme a los criterios de interpretación ampliados en la Ley Modelo y la Convención sobre las comunicaciones

⁷⁵⁵ SHEHATA, I. (2019). “Smart Contracts...”, *cit.*, p. 5.

⁷⁵⁶ La expresión “acuerdo por escrito” denotará una cláusula compromisoria incluida en un contrato o un compromiso, firmados por las partes o contenidos en un canje de cartas o telegramas

⁷⁵⁷ Artículo VII, numeral 4.

⁷⁵⁸ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2017). *Notas técnicas...*, *cit.*, p. 6.

⁷⁵⁹ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2011). *La solución por vía informática de controversias surgidas a raíz de operaciones transfronterizas de comercio electrónico: cuestiones que deberán examinarse para elaborar un marco global que rija la solución de controversias por vía informática (ODR)*, Viena, p. 12. Disponible en: https://uncitral.un.org/es/working_groups/3/online_dispute (fecha de consulta: 30 de enero de 2021).

electrónicas. Desde luego, se trata de una interpretación liberal de la Convención de Nueva York⁷⁶⁰, Sin embargo, ello no impide que Estados con una interpretación más restrictiva nieguen la validez de la misma, así que, a pesar de que sea viable, para tener mayor seguridad jurídica se deberá dejar constancia del acuerdo y de la sentencia por escrito. Por ello, plataformas como Codelegit y Mattereum son conscientes de la inestabilidad jurídica de los contratos inteligentes y la posibilidad de que el acuerdo arbitral solo en código no cumpla con el requisito del artículo 2 de la convención de Nueva York y, por ello, han establecido que el contrato debe contar con un acuerdo redactado en lenguaje natural.

En cuanto al reconocimiento, el artículo 4 de la convención de Nueva York establece que, la parte que pida el reconocimiento y la ejecución deberá presentar el laudo original debidamente autenticado o una copia de ese original que reúna las condiciones requeridas para su autenticidad⁷⁶¹. Si la sentencia no estuviere en un idioma oficial del país donde se pretende reconocer, la parte que la solicite deberá proporcionar una traducción certificada oficial o jurada⁷⁶². De manera similar, el artículo 35.2 de la Ley Modelo de arbitraje estipula que la parte que busque hacer cumplir el laudo debe suministrar el original o copia del mismo. Si el laudo no estuviera redactado en un idioma oficial del Estado en que se pretende hacer cumplir el juez puede solicitarle a la parte que presente una traducción al idioma oficial.

No está claro cómo puede haber una copia original del laudo, ya que el mismo se agrega a la cadena de bloques y es accesible para todos⁷⁶³. Sin embargo, advierte BANSAL que, Blockchain es a prueba de manipulaciones y si se agrega a la cadena estaría certificado en sí mismo. De la misma forma, si la decisión está en código de ordenador, tendrá que traducirse al idioma natural. En cambio, si esta se introduce en el código del contrato inteligente, se hace con el objetivo de que se pueda ejecutar automáticamente, con lo cual su cumplimiento estaría garantizado y no habría necesidad

⁷⁶⁰ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2011). *La solución por vía..., cit.*, p. 9.

⁷⁶⁰ Artículo IV convención de Nueva York.

⁷⁶¹ Artículo IV convención de Nueva York.

⁷⁶² Artículo IV convención de Nueva York.

⁷⁶³ BANSAL, R. (2019). "Enforceability of Awards from Blockchain Arbitrations in India", *Kluwer Arbitration Blog*. Disponible en: <http://arbitrationblog.kluwerarbitration.com/2019/08/21/enforceability-of-awards-from-blockchain-arbitrations-in-india/> (fecha de consulta: 1 de febrero de 2021).

de solicitarlo en sede judicial, como acertadamente señala ORTOLANI, Blockchain permite que el sistema arbitral sea autoaplicable, con lo cual evita, en gran medida los procedimientos de reconocimiento y ejecución mediante los cuales los tribunales estatales ejercen cierto control sobre el arbitraje⁷⁶⁴. No obstante, si la decisión afecta a hechos que suceden por fuera de Blockchain, no habría necesidad de escribirlo en lenguaje de programación, porque el código no tendría que ejecutarlo. El laudo puede estar escrito en idioma natural y solicitarse su ejecución. En resumen, a pesar de todos los obstáculos aparentes que podrían aparecer en el camino para reconocer una decisión dictada a través de las plataformas Blockchain de resolución de controversias, creemos que, si la sentencia cumple los requisitos mínimos establecidos por la ONU a través de la Convención de Nueva York y la Ley Modelo de Arbitraje, ello significa que el fallo sería ejecutable internacionalmente.

Ahora bien, como quiera que hay duda acerca de la validez legal del contrato inteligente, al menos por ahora, las partes deberían celebrar, por seguridad, acuerdos tradicionales de respaldo que acompañen al código de contrato inteligente. Es importante dejar claro que, el reconocimiento del laudo a través de estos mecanismos se hace mediante instituciones tradicionales y centralizadas, en la cual las partes deben ser identificadas, de tal manera que, si apreciamos el entorno libertario en el cual se desarrolla la tecnología, no sabemos si puedan resultar atractivo para los usuarios de la misma. De todas formas, estas soluciones han surgido desde el mismo entorno de Blockchain y, quizás, ello sea una aceptación por parte de la comunidad que dicha tecnología necesita de actores tradicionales y centralizados para poder generar confianza.

2.2 Costos

El reconocimiento y ejecución de laudos arbitrales por vía judicial supone un obstáculo en sí mismo. La parte que pretende hacerlo valer debe someterse a procedimientos lentos y costosos que irían en contraposición de las bases ideológicas de la tecnología Blockchain. Es cuestionable si este mecanismo es conveniente para

⁷⁶⁴ ORTOLANI, P. (2019). "The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads", *Uniform Law Review*, Vol. 24, No. 2, p. 430. Disponible en: <https://doi.org/10.1093/ulr/unz017> (fecha de consulta: 14 de marzo de 2020).

contratos de escaso valor económico, ya que tal reconocimiento supondría incluso que el costo de ejecutar el laudo sea superior a la suma en controversia⁷⁶⁵.

3. Consideraciones

A lo largo de este capítulo nuestro objetivo ha sido, fundamentalmente, tratar de dar respuesta a cómo resolverán las partes anónimas las disputas, si ningún método es lo verdaderamente suficiente.

Antes de dar respuesta a esta cuestión, es importante mencionar, que es clave que las partes establezcan desde el principio el método de resolución de disputa⁷⁶⁶, pues dada la naturaleza de la tecnología, ya sabemos los problemas técnicos para revertir una operación.

Es evidente que la justicia tradicional tiene un alcance limitado para resolver disputas entre partes anónimas. En primer lugar, si se desconoce la identidad de las partes, ello implica que, nociones como jurisdicción y ley aplicable no se puedan materializar. Luego, entonces, si los contratantes desean que sus disputas sean resueltas a través de esta vía, necesariamente tendrán que identificarse y permitir que instituciones tradicionales y centralizadas dirima el litigio.

Por otra parte, los métodos alternativos de resolución de controversias descentralizados y de colaboración colectiva o *Crowdsourcing* (CODR) presentan problemas de justicia y equidad, las decisiones son motivadas mediante incentivos económicos, lo que genera preocupación. No obstante, es un sistema rápido, barato y eficiente, que puede llegar a ser el más adecuado para disputas de escaso valor económico, ya que “los costos y la complejidad de los procedimientos judiciales son desproporcionados con respecto a los valores en disputa”⁷⁶⁷. En otras palabras, los costos legales superan el monto del litigio, lo cual, en muchas ocasiones implica, que la parte afectada decida no iniciar una reclamación. A lo mejor, este no sea el recurso más

⁷⁶⁵ COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2011). *La solución por vía...*, cit., p. 4.

⁷⁶⁶ NORTON ROSE FULBRIGHT (2019). “Blockchain dispute risks for banks”. Disponible en: <https://www.nortonrosefulbright.com/es-es/knowledge/publications/3fb55e09/blockchain-dispute-risks-for-banks> (fecha de consulta: 20 de febrero de 2021).

⁷⁶⁷ ORTOLANI, P. (2016). “Self-Enforcing ...”, cit., p. 628.

equitativo, con que cuenten las partes para resolver sus disputas de bajo impacto, pero si el primero⁷⁶⁸ o el único, más aún, si se trata de controversias entre partes no identificadas, puesto que ni el arbitraje legalmente vinculante, ni la justicia tradicional pueden ofrecer resolver litigios entre partes anónimas. Sin embargo, para que estos mecanismos operen de manera justa y equitativa es imprescindible que haya respuestas regulatorias globales que concilien las características de Blockchain con el debido proceso y la equidad, aunque ello suponga que la tecnología tenga que ceder un poco de sus cualidades más atractivas. En todo caso, estas plataformas se encuentran en sus estados iniciales de desarrollo, no sabemos cómo funcionarán en el futuro⁷⁶⁹. Quizás, su respuesta, por ahora, dependa de los trabajos adelantados por la CNUDMI para la resolución de controversias vía internet, para las operaciones de comercio electrónico internacional y de estas plataformas, porque puede que estén allanando el camino hacia nuevas formas de resolución de disputas.

En cuanto al arbitraje internacional, a pesar de que se presente como el más adecuado, existen preocupaciones sobre reconocimiento y validez en Estados con una interpretación más restrictiva de la convención de Nueva York, ¿Entonces, ¿cuál es el mejor método? En estos momentos la respuesta depende de la cuantía del litigio, porque cuanto más compleja sea la transacción y más dinero esté involucrando, las partes querrán tener más certeza que sus disputas serán resueltas de forma adecuada, por lo tanto, no existe un único método viable. CODR se aplicaría a operaciones o reclamos menores y simples donde no estén comprometidas grandes sumas de dinero. Sin embargo, para las cuestiones más complejas que requieran cierto nivel de especialización es más conveniente el uso del arbitraje internacional o los métodos tradicionales, aunque este último se presente como menos atractivo dada su lentitud. También habrá que ver si los usuarios están dispuestos a resolver disputas de gran envergadura a través del arbitraje virtual en Blockchain. Lógicamente, se tendrán que relajar características como el anonimato. Asimismo, por lo menos por ahora, puede que las partes necesiten celebrar acuerdos tradicionales para que no tenga problemas para la aplicación del arbitraje en relación de su validez con la convención de Nueva York.

⁷⁶⁸ RABINOVICH-EINY, O. & KATSH, E. (2019). “Blockchain...”, *cit.*, p. 58, ODR quizás sean la única opción que tengan las personas que se encuentren anónimas.

⁷⁶⁹ JEVREMOVIĆ, N. (2019) “2018: In Review: Blockchain Technology and Arbitration”, Kluwer Arbitration Blog. Disponible en: <http://arbitrationblog.kluwerarbitration.com/2019/01/27/2018-in-review-blockchain-technology-and-arbitration/> (fecha de consulta: 1 de abril de 2021).

Para finalizar, hemos mencionado anteriormente que la tecnología Blockchain y sus métodos de resolución de disputas se encuentran en pleno desarrollo, actualmente no existe ni siquiera una estandarización de la industria. Ahora bien, es de esperar, que a medida que vaya creciendo la tecnología, los usuarios exijan métodos de resolución de disputas justos y que se adapten al entorno. Sin unas reglas claras de gobernanza, no creemos que haya una expansión y adopción masiva de la tecnología Blockchain.

CAPÍTULO QUINTO

BLOCKCHAIN Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

CAPITULO QUINTO: BLOCKCHAIN Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

I.BLOCKCHAIN Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

1. Introducción

El 25 de mayo de 2018 entró en vigor el Reglamento General de protección de datos⁷⁷⁰ (RGPD), el cual se diseñó con el propósito de empoderar a las personas, concediéndole más control y seguridad sobre el uso de sus datos y también con el objetivo de unificar la legislación sobre protección de datos y privacidad al interior de la Unión Europea⁷⁷¹.

El Reglamento es una norma tecnológicamente neutral, en el sentido que establece los principios y requisitos generales de protección de datos, pero no especifica concretamente ninguna tecnología o técnica para implementar los principios y requisitos legales que introduce⁷⁷². No obstante, se concibió con un control central en mente, pues asume que el tratamiento y procesamiento de los datos siempre estará centralizado. Pero las cadenas de bloques a menudo se desarrollan de forma descentralizada, mediante la distribución de cada transacción por toda la red, lo que desafía los conceptos fundamentales del RGPD.

En esta sección, debido a la reducida literatura que se ha ocupado en nuestra lengua de abordar la protección de datos en relación con la tecnología Blockchain, nos proponemos a analizar los desafíos que representa el cumplimiento del RGPD, por parte de las cadenas de bloques públicas. Habida cuenta de que para las redes privadas o autorizadas es menos problemático ajustarse al Reglamento, y más específicamente

⁷⁷⁰ También llamado en esta sección indistintamente como el Reglamento.

⁷⁷¹ CORRALES, M., JURCYS, P. & KOUSIOURIS, G. (2019). "Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework" *Legal Tech, Smart Contracts and Blockchain*, (Dirs. CORRALES, M., FENWICK, M., & HAAPIO, H.), Ed.: Springer Nature, Singapur, p. 192.

⁷⁷² MOEREL, L. (2019). "Blockchain and Data Protection" *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, p. 225.

porque como razonablemente advierte MOREL, “muchos de los argumentos expuestos en el contexto de las cadenas de bloques sin permisos (como Bitcoin o Ethereum) pierden su validez en el contexto de las cadenas de bloques con permiso”⁷⁷³. En realidad, solo las cadenas públicas son descentralizadas y transparentes.

Por tanto, el presente capítulo tiene por objetivo analizar las principales tensiones entre la tecnología Blockchain y el Reglamento General de Protección de Datos. Para ello, primero delimitaremos el concepto de dato según el RGPD. Luego, pasaremos a discutir si la clave pública y el *hash*, constituyen o no datos personales; posteriormente, abordaremos los tipos de datos que se almacenan en una cadena de bloques. Asimismo, discutimos los desafíos de los derechos de los interesados que supone Blockchain, la tensión entre los principios de minimización de datos y limitación del plazo de conservación y finalmente abordamos la cuestión acerca de quién es el responsable del tratamiento en una red abierta y distribuida.

2. Definición de dato personal a la luz del RGPD

Es imperativo delimitar el concepto de lo que se considera datos personales, ya que con ello se determina el alcance material de las obligaciones impuestas en el RGPD⁷⁷⁴. El ámbito de aplicación del Reglamento se circunscribe solo a los datos que califican como personales, quedando fuera de su alcance los datos anónimos⁷⁷⁵. El artículo 4.1 del RGPD define datos personales como “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente,

⁷⁷³ MOEREL, L. (2019). “Blockchain and...”, *cit.*, p. 221.

⁷⁷⁴ WONG, B. (2019). “Delimiting the concept of personal data after the GDPR”, *Legal Studies*, Vol. 39, No. 3, p. 517. Disponible en: <https://www.cambridge.org/core/journals/legal-studies/article/abs/delimiting-the-concept-of-personal-data-after-the-gdpr/20758F3E090F79032F0A41C5843E82D9> (fecha de consulta: 16 de junio de 2021). El ámbito material de del RGPD se circunscribe según su artículo 2.1 a “al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

⁷⁷⁵ Señala el artículo 2.2 que el reglamento no será aplicable “a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención”. En STJUE, Sala 3ª, de 9 de junio de 2020, Asto: C-272/19, VQ / Land Hessen EU:C:2020:535, apartado 68. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-272/19> (fecha de consulta: 10 de junio de 2021) el TJUE advirtió que dicho artículo constituye una excepción a la definición muy amplia del ámbito de aplicación de ese Reglamento enunciada en su artículo 2, apartado 1, y que, por lo tanto, debe interpretarse de manera restrictiva.

en particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”

La definición de datos personales fue examinada en un dictamen no vinculante⁷⁷⁶ emitido por el Grupo de Trabajo del Artículo 29⁷⁷⁷ (al que llamaremos también Grupo de Trabajo), un órgano consultivo de la Unión Europea en materia de protección de datos, bajo la vigencia de la Directiva de protección de datos de 1995. Si bien la definición de datos personales de la Directiva del 95 y la del RGPD pueden diferir en algunos puntos⁷⁷⁸, en realidad guardan muchas semejanzas entre sí. Como acertadamente concluye WONG⁷⁷⁹, son estructuralmente similares, ya que ambas definiciones establecen dos requisitos fundamentales para que la información pueda considerarse como datos personales:

i. La información debe estar relacionada con una persona física;

ii. Que esté viva y

iii. Esa persona debe ser identificable a partir de esa información.

Ello comporta que, tanto la jurisprudencia del TJUE, como las guías de interpretación que abordan la definición bajo la Directiva, siguen siendo relevantes bajo

⁷⁷⁶ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007 sobre el concepto de datos personales*. Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf (fecha de consulta: 17 de junio de 2021).

⁷⁷⁷ El grupo de trabajo del artículo 29 fue creado por la Directiva de 95/46/CE. Está conformado por las Autoridades de Protección de Datos de los Estados miembros, el Supervisor Europeo de protección de Datos y la Comisión Europea, véase APCPD. (2018). “Que es y quienes forman el Grupo de trabajo del artículo 29”. Disponible en: <https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/> (fecha de consulta: 23 de abril de 2022).

⁷⁷⁸ Advierte en la doctrina ARIAS-POU, M. (2016). “Definiciones a efectos del Reglamento General de Protección de Datos”, *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, (Dirs. PIÑARMAÑAS, J), Ed.: Reus, p. 118. que, “el reglamento actualiza el listado de ejemplos que recogía la Directiva para determinar qué datos hacen identificable a una persona”.

⁷⁷⁹ WONG, B. (2019). “Delimiting the concept...”, *cit.*, p. 519, asimismo, SANTOS-MORÓN, M. J. (2020). “Tratamiento de datos, sujetos implicados, responsabilidad proactiva”, *Protección de datos personales*, (Dirs. GONZÁLEZ- PACANOWSKA, I. & CASTILLA-BAREA, M.), Ed.: Tirant lo Blanch, p. 24, señala que el concepto de dato personal no ha variado respecto al de la Directiva del 95.

el régimen del RGPD. Así lo concluyó la abogada general JULIANE KOKOTT⁷⁸⁰, quien señaló que la definición no resulta afectada. No obstante, se debe tener cuidado, ya que los cambios introducidos en el RGPD impactan directa e indirectamente la interpretación del significado de datos personales⁷⁸¹.

El dictamen del grupo de trabajo del artículo 29 articula en 4 elementos el concepto de datos personales:

- i.Toda información;
- ii.Sobre una persona;
- iii.Identificada o identificable y
- iv.Persona física.

A continuación, analizaremos de que trata cada elemento.

2.1 Toda información.

El documento aclara que la intención del legislador europeo es darle un sentido amplio al concepto de datos personales, lo que supone una interpretación amplia de su significado. Se explica que el concepto de datos personales incluye todo tipo de información, cualquiera que sea su naturaleza (objetiva o subjetiva), contenido (personal,

⁷⁸⁰ En este sentido, así se advirtió en el punto 3 de las CONCLUSIONES DE LA ABOGADO GENERAL JULIANE KOKOTT en el caso STJUE, Sala 2ª, de 20 de diciembre de 2017, Asto: C-434/16, Peter Nowak/ Data Protection Commissioner, EU:C:2017:582. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-434/16&td=ALL> (fecha de consulta 10 de febrero de 2022). “Si bien la Directiva de protección de datos será sustituida próximamente por el Reglamento general de protección de datos, que aún no ha entrado en vigor, la definición de datos personales no resulta afectada. Por lo tanto, esta petición de decisión prejudicial también resulta relevante para la aplicación futura del Derecho de la Unión en materia de protección de datos”. En la misma línea advierten la AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2018). *Manual de legislación europea en materia de protección de datos*, pp 40. Disponible en: <https://fra.europa.eu/es/publication/2020/manual-de-legislacion-europea-en-materia-de-proteccion-de-datos-edicion-de-2018> (fecha de consulta: 1 de junio de 2021) que, “Esa jurisprudencia preexistente sigue siendo pertinente y válida para la interpretación y aplicación de los principios de protección de datos de la UE, en la medida en que los principios y conceptos fundamentales de la Directiva sobre protección de datos se mantuvieron en el RGPD”.

⁷⁸¹ WONG, B. (2019). “Delimiting the concept...”, *cit.*, p. 519.

familiar, sensible, pública), o formato, lo que implica que, independientemente la forma en cómo se presente un dato, este potencialmente puede convertirse en dato personal.

En concordancia con el punto de vista del dictamen, En Nowak contra Data Protection Commissioner, el TJUE señala que, el empleo de la frase “toda información” refleja el objetivo del legislador europeo de atribuirle al concepto de datos personales “un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión”⁷⁸².

2.2 La información debe versar sobre una persona

El grupo de Trabajo del Artículo 29 considera que la información versa sobre una persona cuando se refiere a ella⁷⁸³. En muchas ocasiones puede ser obvio establecer esa relación, como, por ejemplo, las imágenes filmadas en video de una persona para una entrevista, mientras que en otras situaciones tal conexión no es tan evidente. Puede existir un vínculo indirecto, pues el dato no se relaciona con un individuo, sino con un objeto, el cual pertenece o está bajo la influencia de esa persona. Por ejemplo, el cuaderno de anotaciones de un mecánico contiene información sobre revisiones pasadas de un coche. Dicha información se asocia a una matrícula que, se vincula a su propietario, por lo que, en los casos en los que el mecánico haga una conexión entre el automóvil y su dueño, por ejemplo, para facturar, dicha información versará sobre el propietario.

La guía señala, además, que para que la información pueda relacionarse con una persona, debe satisfacerse alguno de los siguientes elementos: contenido, propósito o resultado. La presencia de cualquiera de estos elementos podría convertir cualquier información en dato personal, pues el dictamen aclara que deben considerarse como condiciones alternativas y no acumulativas.⁷⁸⁴

⁷⁸² STJUE, Sala 2ª, de 20 de diciembre de 2017, apartado 34.

⁷⁸³ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, Op. Cit. p. 9.

⁷⁸⁴ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, Op. Cit. pp. 9-12.

i.*Contenido*. El elemento contenido significa que, la información versa sobre esa persona cuando se refiere a esa persona, como, por ejemplo, los resultados de una analítica se refieren al paciente.

ii.*Finalidad*. La información se relaciona con una finalidad cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera, o influir en la situación o el comportamiento de una persona.

iii.*Resultado*. Por último, señala el dictamen que el elemento resultado se satisface cuando el uso de la información⁷⁸⁵ es susceptible de tener un impacto en los derechos y los intereses de una persona en particular. Basta con que el individuo pueda ser tratado de manera diferente por otras personas como resultado del tratamiento de tales datos.

2.3 La persona ha de estar identificada o identificable

En cuanto al tercer elemento, observa el dictamen que, un individuo se considera identificado cuando dentro de un grupo se puede distinguir de los demás miembros, e identificable cuando, aunque la persona aún no haya sido posible identificarla, es probable hacerlo⁷⁸⁶. De modo que, no es necesaria la identificación del interesado, sino que basta con que sea potencialmente posible hacerlo. El grupo de trabajo es claro en precisar que la identificación no solo hace referencia a la posibilidad de restablecer el nombre o la dirección de una persona, sino que también incluye la identificabilidad potencial por singularización, vinculabilidad o inferencia⁷⁸⁷.

i.*Singularización*: hace referencia al riesgo de extraer de un conjunto de datos atributos que identifican a una persona;

⁷⁸⁵ WONG, B. (2019). “Delimiting the concept...”, *cit.*, p. 526.

⁷⁸⁶ TEPERDJIAN, R. (2020). “The Puzzle of Squaring Blockchain with the General Data Protection Regulation”, *jurimetrics*, Vol. 60, No. 3., p. 25. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3638736 (fecha de consulta: 20 de junio de 2021). Véase también UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, *Op. Cit.* pp. 12-13.

⁷⁸⁷ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014), *Dictamen 05/2014 sobre técnicas de anonimización*. Disponible en <https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf> (fecha de consulta: 17 de junio de 2021).

ii. *Vinculabilidad*: consiste en la posibilidad de vincular al menos dos atributos de una misma persona o grupo, ya sea mediante la misma fuente de datos o de fuentes distintas. Señala el Grupo de Trabajo que si un atacante puede establecer (por ejemplo, mediante un análisis de correlación) que dos registros están asignados a un mismo grupo de personas, pero no se pueden singularizar a las personas en este grupo, entonces la técnica empleada es resistente a la singularización, pero no a la vinculabilidad.

iii. *Inferencia*: señala el Grupo de trabajo que la inferencia es el riesgo de deducir con una probabilidad significativa el valor de un atributo a partir de otros atributos, como, por ejemplo, señala el estudio del Parlamento Europeo donde un conjunto de datos no hace referencia a Angela Merkel, sino a la Canciller de Alemania de la década de los 20000, por lo que su identidad se puede inferir⁷⁸⁸.

La identificación puede ser directa o indirecta, y se efectúa mediante datos concretos, denominados como identificadores, los cuales “tienen una relación privilegiada y muy cercana con una determinada persona”⁷⁸⁹. Menciona el dictamen que un identificador directo, puede ser, por ejemplo, el nombre y sus apellidos, mientras que, un identificador indirecto, se da en los casos en los que haya que cruzar datos, pues, si bien a primera vista, no se puede singularizar a una determinada persona, es posible que sea identificable, porque si esos datos se combinan con otros, es probable establecer su identidad y distinguirla del resto de personas⁷⁹⁰. Cabe destacar que, en Breyer contra Bundesrepublik el TJUE⁷⁹¹ consideró que, “no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona”, con lo cual puede ser considerado como un medio razonable de ser utilizado.

⁷⁸⁸ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?* pp. 21-22. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf) (fecha de consulta: 1 de junio de 2021).

⁷⁸⁹ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, Op.Cit., p. 13.

⁷⁹⁰ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, Op. Cit., p. 14.

⁷⁹¹ STJUE, Sala 2ª, de 19 de octubre de 2016, Asto: C-582/14, Patrick Breyer/ Bundesrepublik Deutschland, EU:C:2016:779, apartado 43. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-582/14&td=ALL> (fecha de consulta: 15 de junio de 20202).

Es imperativo señalar que el considerando 26 del RGPD (al igual que la Directiva del 95), señala claramente que, para determinar si una persona física es identificable “deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física”, asimismo aclara que para determinar si hay posibilidad razonable de que se utilicen medios para identificar a una persona física “deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos”, de tal manera que, una persona puede que no sea identificable al momento de la recopilación, no obstante, más tarde en el tiempo, esa persona se puede identificar, en virtud del progreso tecnológico.

2.4 Persona física

El último componente de la definición de datos personales es persona física, y hace referencia a que las normas de protección de datos se circunscriben solamente a los seres humanos que se encuentren vivos⁷⁹². Por tanto, el Reglamento no se aplica a los datos relativos a las personas jurídicas⁷⁹³ o personas fallecidas, ya que su objetivo es garantizar “el respeto de los derechos fundamentales reconocidos a las personas físicas”⁷⁹⁴. No obstante, si la información de los sujetos a los cuales no aplica el RGPD identifica indirectamente a personas físicas, entonces sí estará sujeta a la protección de datos⁷⁹⁵. Por ejemplo, los datos relativos a una persona fallecida pueden ser, como advierten VOIGT y otros, datos personales para sus descendientes en el caso de enfermedades hereditarias.⁷⁹⁶

⁷⁹² UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007), *Dictamen 4/2007...*, *Op. Cit.*, p. 24.

⁷⁹³ STJUE, Sala 1ª, 10 de diciembre de 2020, Asunto: C-620/19, Land Nordrhein-Westfalen/ D.-H. T, EU:C:2020:649, apartado 41. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-620/19&language=ES> (fecha de consulta: 1 de junio de 2021).

⁷⁹⁴ STJUE, Sala 1ª, 10 de diciembre de 2020, apartado 45. Asimismo, la AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2018). *Manual...*, *Op. Cit.* p. 98 señala que, la Directiva sobre la privacidad y las comunicaciones electrónicas sí protege la confidencialidad de las comunicaciones y los intereses legítimos de las personas jurídicas en relación con el incremento de la capacidad de almacenamiento y tratamiento automatizado de datos relativos a abonados y usuarios.

⁷⁹⁵ GOLDEN DATA LAW. (2018). “Material scope of EU data protection law”. Disponible en: <https://medium.com/golden-data/material-scope-of-eu-data-protection-law-39ecd18f7ff6> (fecha de consulta: 1 de junio de 2021).

⁷⁹⁶ VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general data protection regulation (GDPR). A Practical Guide*, Springer International Publishing, Cham, Switzerland, p. 11.

3. Anonimización y seudonimización

En la presente sección responderemos a la pregunta de si la clave pública y la función *hash* son técnicas de anonimización o si, por el contrario, son datos seudónimos, lo que los convertiría en datos personales y, por tanto, estarían bajo el ámbito de aplicación del Reglamento. Para ello, primero abordaremos los conceptos de anonimato y seudonimización de manera general, a la luz del RGPD, y luego debatimos si las técnicas en comento califican o no como datos personales.

3.1 Anonimización

El RGPD adopta una posición binaria entre datos personales y no personales y somete al ámbito de su aplicación solo al primero⁷⁹⁷, de modo que, no aplica a la información no relacionada con una persona física identificada o identificable⁷⁹⁸. No obstante, como tuvimos oportunidad de ver, el concepto de datos personales es bastante amplio⁷⁹⁹ y sin duda, con el rápido crecimiento de la informática, como señala PURTOVA, está destinado a expandirse aún más⁸⁰⁰. Por lo que, existe un margen muy estrecho, para que un dato pueda ser considerado como anónimo.

Acertadamente, y a diferencia de la interpretación absoluta que había introducido el Grupo de trabajo en el Dictamen sobre técnicas de anonimización, en el cual el anonimato debía ser irreversible⁸⁰¹, el RGPD en el considerando 26, proporciona un

⁷⁹⁷ PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, Op. Cit., p. 14.

⁷⁹⁸ El considerando 26 del RGPD señala que los principios de protección de datos deben aplicarse solo a los datos personales.

⁷⁹⁹ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. (2018). *Blockchain And the GDPR*, p. 10. Disponible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (fecha de consulta 16 de junio de 2021). Véase también UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, Op. Cit., p. 4.

⁸⁰⁰ PURTOVA, N. (2018). "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10, No. 1, p. 41. Disponible: <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> (fecha de consulta: 16 de junio de 2021).

⁸⁰¹ Al respecto la UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014...*, Op. Cit., p. 7, al momento de hacer un análisis jurídico de la anonimización señala que, "La anonimización puede ser el resultado de un tratamiento de datos personales realizado para **impedir de forma irreversible** la identificación del interesado". Subrayado y negrita fuera del texto. De igual forma, el EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. (2018). *Blockchain...*, Op. Cit., p. 19, advierte que "el listón de lo que se considera anonimizado está muy alto. No sólo debe ser lo suficientemente buena como para que sea imposible identificar a una persona física a través de todos y cada uno de los medios "razonablemente probables", sino que además el proceso debe ser irreversible".

enfoque basado en el riesgo, pues en contraste con el Dictamen 05/2014, acepta que el proceso de anonimización no es absoluto, de tal manera que, para establecer la identificabilidad se deben tener en cuenta: los costes y el tiempo necesarios para la identificación, la tecnología disponible en el momento del tratamiento y los avances tecnológicos⁸⁰². De manera análoga, el TJUE en el caso Breyer contra Bundesrepublik determinó que, el riesgo de identificación es insignificante si implica un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos⁸⁰³.

El objetivo del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados⁸⁰⁴, esto es, es evitar que se reidentifique a una persona. Sin embargo, el RGPD prevé que ninguna técnica de anonimización es absoluta, pues siempre van a existir riesgos residuales de reidentificación⁸⁰⁵, por lo que advierte que, se debe tener en cuenta tanto la tecnología disponible en el momento del tratamiento, como los avances tecnológicos⁸⁰⁶. El Grupo de Trabajo del artículo 29 en la misma línea, ha advertido que, la anonimización es cada vez más difícil de conseguir con el avance de la tecnología informática moderna y la disponibilidad ubicua de información⁸⁰⁷, de manera que no es difícil encontrar que un dato sea anónimo al momento de su recopilación, pero puede convertirse en personal⁸⁰⁸, en virtud del paso del tiempo. Por ello, se ha alertado de la necesidad de revisar

⁸⁰² Considerando 26 del RGPD.

⁸⁰³ STJUE, Sala 2ª, de 19 de octubre de 2016, apartado 41.

⁸⁰⁴ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, p. 2. Disponible en: <https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf> (fecha de consulta: 20 de junio de 2021).

⁸⁰⁵ Opinan de manera similar la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2016). *Orientaciones...*, *Op. Cit.*, p. 7, incluso una parte de la doctrina académica opina que, el anonimato absoluto e irreversible ya no es posible o es un objetivo inalcanzable, véase PURTOVA, N. (2018). "The law of everything...", *cit.*, p. 77, NARAYANAN, A., SHMATIKOV, V. (2010). "Myths and fallacies of" personally identifiable information". *Communications of the ACM*, Vol. 53, No. 6, p. 26. Disponible en: https://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf (fecha de consulta: 16 de junio de 2021).

⁸⁰⁶ Considerando 26 del RGPD.

⁸⁰⁷ Véase EUROPEAN UNION, ARTICLE 29 DATA PROTECTION WORKING PARTY (2013) *Opinion 03/2013 on purpose limitation*, p. 31. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (fecha de consulta: 23 de junio de 2021). Asimismo, UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, *Op. Cit.*, p. 17, señala que, "debe tenerse en cuenta el grado de avance tecnológico en el momento del tratamiento y su posible desarrollo en el período durante el cual se tratarán los datos. Puede que la identificación no sea factible hoy con el conjunto de los medios que puedan ser razonablemente utilizados en la actualidad. Si lo previsto es que los datos se conserven durante un mes, puede que no sea factible adelantar la identificación para que esté terminada dentro del «período de vida» de la información y, por lo tanto, esa información no debe considerarse como datos personales. Ahora bien, si el período de conservación previsto es de diez años, el responsable del tratamiento debe barajar la posibilidad de que la identificación pueda producirse al cabo de nueve años, con lo que adquiriría en ese momento la categoría de datos personales"

⁸⁰⁸ PURTOVA, N. (2018). "The law of everything...", *cit.*, p. 44.

periódicamente las medidas técnicas y adaptarlas a los avances tecnológicos. En efecto, un estudio llevado a cabo en 2019 por ROCHER y otros, arrojó que los datos anonimizados nunca son totalmente anónimos. Dicha investigación reveló que, con un conjunto de datos, utilizando 15 atributos demográficos, es suficiente para reidentificar al 99.98% de los estadounidenses⁸⁰⁹.

En definitiva, los constantes avances de procesos como el análisis de datos, los incentivos económicos y la facilidad de hallar información disponible sobre millones de personas, provenientes de una vida “inteligente” gracias a la omnipresencia de dispositivos conectados como, teléfonos inteligentes, Smart Tv, Robot de limpieza, Relojes inteligentes, luces inteligentes, coches inteligentes, asistente voz etc., de tal forma que cualquier información se relaciona con una persona, por tanto, “el análisis de Big Data hace que la distinción binaria entre información identificable y no identificable carezca de sentido”⁸¹⁰, ya que cuanto mayor sea la cantidad de datos disponibles, más informativos serán dichos datos y será más fácil la identificación⁸¹¹.

Asimismo, a lo largo de los años ha habido muchos casos en los cuales se ha dejado al descubierto los problemas de seguridad a los que se enfrentan los datos anonimizados, como consecuencia de técnicas incompletas o erróneas ⁸¹². Por ejemplo, en el año 2013 la Comisión de Taxis y Limusinas de Nueva York, a petición de un ciudadano, gracias a una solicitud amparada por la *Freedom of information Act*, publicó de forma anonimizada la base de datos de todos los viajes de la ciudad (alrededor de 173 millones). No obstante, las rutas de viajes de celebridades como Bradley Cooper o Jessica Alba quedaron al descubierto. Los paparazis de Nueva York suelen tomar fotografías de celebridades y muchas veces dichas fotos muestran el número de matrícula de los taxis en los cuales se movilizan. Usando marcas de tiempo de las imágenes y las descripciones

⁸⁰⁹ ROCHER, L., HENDRICKX, J. M., & DE MONTJOYE, Y. A (2019). “Estimating the success of re-identifications in incomplete datasets using generative models”, *Nature Communications*, Vol. 10, No. 1. Disponible en: <https://www.nature.com/articles/s41467-019-10933-3> (fecha de consulta: 22 de agosto de 2021).

⁸¹⁰ TENE, O., & POLONETSKY, J. (2013). “Big data for all: Privacy and user control in the age of analytic”, *Northwestern Journal of Technology and Intellectual Property* 258, como se citó en PURTOVA, N. (2018). “The law of everything...”, *cit.* p. 42.

⁸¹¹ TUCKER, P. (2013). Has big data made anonymity impossible?, *Technology Review*, Vol. 166, No. 4. Disponible en: <https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/> (fecha de consulta: 2 de agosto de 2022).

⁸¹² AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021). *10 malentendidos relacionados con la anonimización*, p. 2. Disponible en: <https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf> (fecha de consulta: 2 de agosto de 2021).

donde fueron tomadas las fotografías, el usuario pudo establecer el lugar donde tomaron y dejaron el vehículo, la tarifa que pagaron e incluso la propina que dejaron⁸¹³. De igual forma, un estudio realizado por dos investigadores de la Universidad de Texas, NARAYANAN Y SHMATIKOV, logró que se reidentificaran a algunos clientes que habían participado en un reto de clasificación de películas organizado por Netflix. La plataforma de streaming publicó, anonimizando los datos personales de los participantes, una base de datos de 10 millones de clasificaciones, elaboradas por alrededor de 500 mil usuarios. No obstante, los investigadores compararon los datos anonimizados publicados por Netflix, con información de clasificaciones de películas disponible de forma pública en el portal *Internet Movie Database* (IMDb)⁸¹⁴. El estudio arrojó que se podía saber las aparentes preferencias políticas y otra información potencialmente sensible⁸¹⁵. Con ello se demostró que, el proceso de desanonimización no es complejo y que solo hacen faltas algunos datos para hacerlo, debido a que nuestros hábitos de visualización de películas, lectura de libros, navegación o compra por la web son muy personales⁸¹⁶.

Si bien la Unión Europea no proporciona un estándar de anonimización exitosa per se⁸¹⁷, El Grupo de Trabajo del Artículo 29 en el Dictamen sobre técnicas de anonimización, aborda cuestiones legales y políticas específicas, y revisa descriptivamente una serie de métodos técnicos⁸¹⁸. Recordemos además que señala que para que una técnica de anonimización sea efectiva, debe impedir tres riesgos claves⁸¹⁹:

⁸¹³Véase TROTTER, J.K. (2014). “Public NYC Taxicab Database Lets You See How Celebrities Tip”. Disponible en: <https://www.gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546> (fecha de consulta: 5 de agosto de 2021). Asimismo, Hern, A. (2014). “New York taxi details can be extracted from anonymised data, researchers say”. Disponible en: <https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn> (fecha de consulta: 5 de agosto de 2021), indica que de dicha base de datos también se pudieron extraer datos personales de los taxistas como su lugar de residencia.

⁸¹⁴ NARAYANAN, A., & SHMATIKOV, V. (2008,). “Robust de-anonymization of large sparse datasets”, 2008 *IEEE Symposium on Security and Privacy*, p. 111. Disponible en: <https://ieeexplore.ieee.org/abstract/document/4531148> (fecha de consulta: 16 de junio de 2021).

⁸¹⁵ NARAYANAN, A., & SHMATIKOV, V. (2006). “How to break anonymity of the netflix prize dataset”, arXiv preprint. Disponible en: <https://arxiv.org/abs/cs/0610105> (fecha de consulta: 16 de junio de 2021).

⁸¹⁶ SCHNEIER, B. (2007). “Why 'Anonymous' Data Sometimes Isn't”. Disponible en: <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/> (fecha de consulta: 18 de junio de 2021).

⁸¹⁷ ANDREW, J., & BAKER, M. (2021). “The general data protection regulation in the age of surveillance capitalism”, *Journal of Business Ethics*, Vol. 168, No. 3, p. 572. Disponible en: <https://link.springer.com/article/10.1007/s10551-019-04239-z> (fecha de consulta: 3 de agosto de 2021).

⁸¹⁸ EL EMAM, K., & ALVAREZ, C. (2015). “A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques”, *International Data Privacy Law*, Vol. 5 No. 1. Disponible en: <https://academic.oup.com/idpl/article-abstract/5/1/73/2863828?redirectedFrom=fulltext&login=true> (fecha de consulta: 3 de agosto de 2021).

⁸¹⁹ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014... cit.*, p. 13.

- i. La posibilidad de singularizar a una persona;
- ii. La posibilidad de vincular registros relativos a una persona y;
- iii. La posibilidad de poder inferir información relativa a una persona.

A su vez, aconseja la combinación de dos técnicas de anonimización: la aleatorización y la generalización. Por su parte, la generalización es una técnica que “modifica la veracidad de los datos a fin de eliminar el estrecho vínculo entre los mismos y la persona”⁸²⁰, mientras que la generalización, se trata de una técnica que “generaliza o diluye los atributos de los interesados modificando las respectivas escalas u ordenes de magnitud”, por ejemplo, un país en lugar de una ciudad. El Grupo de Trabajo aclara que ninguna de estas dos técnicas es segura por sí misma, de modo que solo la combinación de ambas puede llegar a ser segura y despersonalizar con éxito los datos⁸²¹. Sin embargo, a la luz de lo anterior, resulta difícil el paradigma de la anonimización, pues siempre hay riesgos residuales, es por ello que el Reglamento reconoce que, si se reduce la vinculabilidad, estamos hablando de datos seudónimos.

3.2 Seudonimización

La seudonimización es una técnica que permite cambiar un dato original por uno seudónimo, por ejemplo, el nombre de una persona, por un alias. A diferencia del anonimato, es un proceso reversible. El artículo 4.5 del RGPD define la seudonimización como “el tratamiento de datos personales de manera tal que, ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable”. Ello significa que, con la seudonimización se puede lograr la reidentificación de los individuos, en la medida en que la información no se destruye,

⁸²⁰ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014... cit.*, p. 13.

⁸²¹ FINCK, M., & PALLAS, F. (2020). “They who must not be identified—distinguishing personal from non-personal data under the GDPR”, *International Data Privacy Law*, Vol. 10, No. 1. Disponible en: <https://academic.oup.com/idpl/article/10/1/11/5802594> (fecha de consulta: 5 de agosto de 2022).

sino que se mantiene por separado, a través del empleo de medidas técnicas y organizativas⁸²².

El Grupo de Trabajo del Artículo 29 en el Dictamen 05/2014⁸²³ determinó que, la seudonimización no constituye anonimización, porque si bien reduce la vinculabilidad de un conjunto de datos con el interesado, siendo una medida de seguridad útil. Advierte que, sigue existiendo una alta probabilidad de identificar a la persona de forma indirecta.

Los datos seudónimos se consideran datos personales⁸²⁴ y le es aplicable el Reglamento, no obstante “su procesamiento comporta menos riesgos para los interesados y se les otorgan ciertos privilegios para incentivar su uso”⁸²⁵. Por ejemplo, el artículo 6.4 del RGPD permite una relajación de la licitud del tratamiento al permitir tratar los datos seudonimizados o cifrados para otro fin con el que se recogieron inicialmente. En definitiva, el Reglamento General de Protección de Datos considera al cifrado como una de las medidas técnicas capaces de reducir los riesgos en el tratamiento de datos⁸²⁶.

II.DATOS ALMACENADOS EN BLOCKCHAIN

Es importante recordar que una de las características fundamentales de funcionamiento de cualquier Blockchain, independientemente de su diseño, es el empleo de dos soluciones criptográficas: la función *hash* y algoritmo *RSA* (criptografía asimétrica)⁸²⁷, con ellas, esta tecnología sustenta su seguridad y logra los requisitos de integridad de los datos y autenticación de identidad de los participantes”⁸²⁸. Las

⁸²² ANDREW, J., & BAKER, M. (2021). “The general data...”, *cit.*, p. 573.

⁸²³ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014...*, *cit.*, p. 22

⁸²⁴ El considerando 26 del RGPD establece que, “Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable”.

⁸²⁵ EDWARDS L (2018) *Law, Policy and the Internet*, Hart Publishing, Oxford, como se citó en EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 17. Es importante subrayar que el considerando 28 del RGPD señala que, la seudonimización reduce los riesgos: “La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos”.

⁸²⁶ Considerando 83 y artículo 32. 1 del RGPD.

⁸²⁷ RAMPONE, F. (2018). “Data Protection in the Blockchain Environment: GDPR is not a Hurdle to Permissionless DLT Solutions”, *Cyberspazio e diritto*, 2018, Vol. 19, No. 61, p. 3. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383619 (fecha de consulta: 20 de agosto de 2021).

⁸²⁸ BACON, J., MICHELS, J. D., MILLARD, C., & SINGH, J. (2018). “Blockchain demystified: a technical and legal introduction to distributed and centralized ledger”, *Richmond Journal of Law & Technology*, Vol. 25, No. 1, p. 5.

identidades de los usuarios se ocultan detrás de las claves públicas, y el *hash* se utiliza para encubrir identificadores personales⁸²⁹, hacer la cadena de bloques a prueba de manipulaciones y proporcionar un medio para hacer referencia única a los datos que se mantienen fuera de la misma⁸³⁰.

La presente sección tiene como objetivo revisar si la función *hash* y la criptografía asimétrica de clave pública califican como datos personales al usarlos en una cadena de bloques, es decir, si los datos en Blockchain están lo suficientemente anonimizados para que no se consideren como datos personales. Para dar respuesta a esta cuestión, primero describiremos a grandes rasgos en qué consiste la función *hash* y la criptografía asimétrica, luego describiremos su aplicación en Blockchain y finalmente procederemos a analizar bajo qué condiciones podrían considerarse o no datos personales de acuerdo a lo establecido en el RGPD.

1. Función *Hash*

Es una función matemática que transforma cualquier dato (frase, nombre, novela, canción, etc.) de longitud variable en una salida alfanumérica de tamaño fijo. Es decir, independientemente del tamaño que tenga la entrada, la salida siempre va a tener la misma longitud. El mismo dato (entrada) siempre se va a convertir en la misma salida, lo que significa que es determinista. Por ejemplo, si generamos el valor de entrada Pablo en la función Sha256, una de las más conocidas porque es la que utiliza la cadena de bloques de Bitcoin⁸³¹, nos va a dar siempre como resultado⁸³²:

Disponible en: <https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf> (fecha de consulta: 27 de agosto de 2021).

⁸²⁹ MANTEGHI, M. (2021). "Blockchain and the European Union's General Data Protection Regulation: from Conflict to "Peaceful" Coexistence?", p. 12. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805647 (fecha de consulta: 16 de agosto de 2021).

⁸³⁰ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FÓRUM. (2018). *Blockchain...*, Op. Cit., p. 21.

⁸³¹ El algoritmo *Hash* de Bitcoin es de 256 Bits, contiene 64 caracteres y cada carácter suma 4 Bits, para un total de 256. Existen distintas funciones *Hash*, Ethereum utiliza la función *Hash* Sha3.

⁸³² Hemos utilizado este generador *Hash* para hacer la conversión disponible en: <https://emn178.github.io/online-tools/sha256.html> (fecha de consulta: 12 de agosto de 2021).



Figura No. 3. Función *hash* de Pablo. Fuente: elaboración propia.

Si modificamos un poco y en lugar de escribir Pablo, escribimos pablo (la p en minúscula), nos va a dar como resultado:

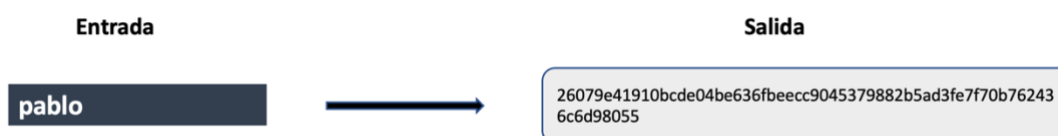


Figura No. 4. Función *hash* de pablo. Fuente: elaboración propia.

Podemos observar que cualquier cambio en la entrada, por muy pequeño que sea, va a generar una variación bastante considerable en la salida, lo que da lugar a un *hash* totalmente distinto. Esta característica permite crear lo que se conoce como una huella digital, dado que garantiza que la entrada original no ha sido modificada⁸³³ o manipulada. En otras palabras, el *hash* sirve como resumen de longitud fija, o resumen inequívoco, de un mensaje⁸³⁴.

La entrada se asocia con la salida, pero a partir de la salida no se puede conocer la entrada original. Esto es lo que se conoce como una función unidireccional, o que no está diseñada a la inversa, lo que significa que, en nuestro ejemplo, se puede saber que la función *hash* de Pablo es la que aparece en la figura No. 3, pero a partir de este resultado no se puede reconstruir que la entrada, que está encubierta, es Pablo.

No obstante, la propiedad determinista hace que “si se conoce el rango de los valores de entrada de la función *hash*, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado”⁸³⁵. Es decir, se pueden adivinar las

⁸³³ RAMPONE, F. (2018). “Data Protection...”, *cit.*, p. 4.

⁸³⁴ NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., & GOLDFEDER, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, Princeton University Press, p. 38.

⁸³⁵ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014...*, *Op. Cit.*, p. 22.

salidas si se conocen las entradas, por ejemplo, imagine que se han filtrado una base de datos (Sha-256) que contiene correos electrónicos. Si queremos saber si nuestro correo electrónico ha sido filtrado, lo único que debemos hacer es comparar nuestra dirección de correo convertida en Sha256, con las direcciones de la filtración. Esto es lo que en informática se conoce como ataque de fuerza bruta, que consiste en pruebas de ensayo y error hasta lograr conocer los valores de descifrado (los valores de salida). Como cuando un hacker que intenta hallar una contraseña, prueba tantas combinaciones de contraseña sea posible, con la esperanza de que una de ellas funcione⁸³⁶. Se considera que lograr esto es muy fácil y extremadamente rápido, en efecto, se puede hacer *hashing*, es decir, convertir todas las direcciones de correo electrónico del mundo en *hash*, tardaría 10 milisegundos y costaría menos de una centésima de centavo⁸³⁷. Por tanto, las verificaciones con datos conocidos, fáciles de saber, como el nombre, correo electrónico, o incluso contraseñas, son susceptibles de reidentificación. Por ejemplo, conocer las contraseñas (normalmente están codificadas con *hash*) de acceso a un sitio web, suele ser “fácil”, dado que, cuando creamos una clave, solemos hacerlo con palabras y caracteres comunes de fácil recordación. Es más, una investigación llevada a cabo por WP ENGINE⁸³⁸, en la cual se utilizó una muestra de 10 millones de contraseñas, arrojó que las 3 contraseñas más comunes son: “123456”, la segunda es “password” (contraseña en español), seguida de “1234567”. Lo que demuestra que se suelen utilizar contraseñas poco seguras y fáciles de adivinar. Los hackers conocen de este hecho y, por este motivo, suelen crear listas con contraseñas populares o palabras de uso común, con combinaciones de números y caracteres más usados, a los cuales les aplican *hash*, y de esta manera, pueden así hallar la contraseña de alguien.

⁸³⁶ “¿Qué es un ataque de fuerza bruta? (Sin fecha) Disponible en: <https://www.avast.com/es-es/c-what-is-a-brute-force-attack#gref> (fecha de consulta: 5 de agosto de 2021).

⁸³⁷ ACAR, G. (2018). “Four cents to deanonymize: Companies reverse hashed email addresses”. Disponible en: https://freedom--to--tinker-com.translate.goog/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=op (fecha de consulta: 7 de agosto de 2021).

⁸³⁸ WP ENGINE. (2022). “Unmasked: What 10 million passwords reveal about the people who choose them”. Disponible en: <https://wpengine.com/resources/passwords-unmasked-infographic/> (fecha de consulta: 10 de agosto de 2022).

Dada la susceptibilidad al ataque de fuerza bruta y ataques de diccionario,⁸³⁹ se han desarrollado técnicas más avanzadas para hacer más resistentes las funciones *hash* a saber, función *hash* con sal y pimienta.

i. *Función hash con sal*: la sal o salazón consiste en agregar a la función *hash* un dato adicional aleatorio, por tanto, no se puede usar un diccionario, lo que reduce la posibilidad de un ataque de fuerza bruta, porque, aunque la entrada “Pablo”, siempre genere la misma salida, si se añade sal, el *hash* que se producirá no será el mismo. En consecuencia, descifrar el valor *hash* requerirá el doble de trabajo⁸⁴⁰. No obstante, el Grupo de Trabajo, en el Dictamen sobre técnicas de anonimización, considera que esta técnica no anonimiza, ya que es posible calcular el valor del atributo oculto tras el resultado de una función *hash* con sal es posible con medios razonables⁸⁴¹.

ii. *Función hash con pimienta*. La pimienta es una secuencia secreta de *bits* que se le agregan a los datos antes de convertirlo en *hash*. Aunque la pimienta funcione de forma similar a la sal, se diferencian en que la sal se almacena con el valor *hash*, mientras que la pimienta esta oculta del valor *hash*. Es decir, se guarda por separado y en secreto⁸⁴², por lo que, es más segura que la sal, porque en caso de una violación de datos el pirata no conoce la pimienta.

1.1 Función *hash* en Blockchain

En una cadena de bloques, el *hash* es empleado para adquirir niveles significativos de seguridad en los datos⁸⁴³, lograr el mecanismo de consenso descentralizado y ofuscar la información. En líneas generales, los valores *hash* son usados como identificadores

⁸³⁹ Es un método de *hacking* que consiste en intentar averiguar una contraseña probando las palabras de los diccionarios.

⁸⁴⁰ Véase LIN, R. (2016). “Salt & Pepper: Spice up your hash!”. Disponible en: <https://medium.com/@berto168/salt-pepper-spice-up-your-hash-b48328caa2af> (fecha de consulta: 10 de septiembre de 2022), KAMINSKY, D. (2021). “Salt The Fries: Some Notes On Password Complexity”. Disponible en: <https://dankaminsky.com/2012/01/05/salt-the-fries-some-notes-on-password-complexity/> (fecha de consulta: 10 de septiembre de 2021).

⁸⁴¹ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014...*, Op. Cit., p. 20.

⁸⁴² Véase “Pepper (cifrado)” (Sin fecha). Disponible en: <https://kripkit.com/pepper-cifrado/> (fecha de consulta: 10 de agosto de 2021), “Pepper (criptografía)”. (Sin fecha). Disponible en: [https://hmong.es/wiki/Pepper_\(cryptography\)](https://hmong.es/wiki/Pepper_(cryptography)) (fecha de consulta: 9 de agosto de 2021).

⁸⁴³ “¿Qué es el Hashing?” (2019). Disponible en: <https://academy.binance.com/es/articles/what-is-hashing> (fecha de consulta: 6 de agosto de 2021).

únicos de los bloques de datos y para cifrar los datos de una transacción. En muchas implementaciones de Blockchain, cada nuevo bloque que se genera se hace partiendo del *hash* del bloque inmediatamente anterior⁸⁴⁴(lo que se conoce como un puntero *hash*, pues apunta al bloque de datos más reciente⁸⁴⁵). Por consiguiente, todos los bloques que la conforman están vinculados cronológicamente⁸⁴⁶, formando de esta forma una cadena de bloques. Esto da como resultado que dicha tecnología sea prueba de manipulaciones⁸⁴⁷, pues si se intenta modificar o eliminar una transacción existente, se alterarían los bloques siguientes, lo que produciría un cambio en el puntero *hash*, que es utilizado como vínculo en el bloque siguiente⁸⁴⁸.

No olvidemos que, para añadir un bloque, los mineros han tenido que gastar suficientes recursos computacionales y energía para resolver el problema matemático, con lo cual, si la información es aceptada como válida por el resto de los nodos, el minero es recompensado⁸⁴⁹.

1.2 La función *hash* y su función en el almacenamiento de datos en Blockchain.

¿Puede la función *hash* anonimizar datos?

Generalmente, los bloques de muchas implementaciones Blockchain almacenan dos tipos de datos: el encabezado del bloque y el contenido del bloque o carga útil. El encabezado de bloque incluye: el número del bloque, el valor *hash* del encabezado del bloque anterior, una representación *hash* de los datos del bloque, una marca de tiempo, el tamaño del bloque y el valor *Nonce* (para las Blockchain que utilizan minería). Por otro lado, el contenido del bloque o carga útil incluye una lista de las transacciones y otros

⁸⁴⁴ “¿Qué hace que una Blockchain sea segura?” (2019). Disponible en: <https://academy.binance.com/es/articles/what-makes-a-blockchain-secure> (fecha de consulta: 6 de agosto de 2021).

⁸⁴⁵ Señala NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., & GOLDFEDER, S. (2016). *Bitcoin and...*, Op. Cit., p. 46, que Un puntero *hash* es simplemente un puntero a donde se almacena cierta información junto con un *hash* criptográfico de la información, lo que permite verificar la integridad de la información.

⁸⁴⁶ MANTEGHI, M. (2021). “Blockchain and...”, cit., p. 3.

⁸⁴⁷ Se necesitaría el consenso del 51% de los nodos para reescribir o modificar los bloques.

⁸⁴⁸ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2010). “Blockchain (II): Conceptos básicos desde la protección de datos”. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos> (fecha de consulta: 16 de agosto de 2021).

⁸⁴⁹ Advierte LIANOS, I., HACKER, P., EICH, S., & DIMITROPOULOS, G. (2019). *Regulating blockchain: technological and legal challenges*, Oxford University Press, p. 8, que, entre más transacciones tenga un bloque más ganará el minero, dado que cuando los usuarios envían dinero, pagan una tarifa de transacción que ellos mismos escogen, cuanto más alta sea, más rápida será procesada.

tipos de datos⁸⁵⁰. El encabezado no suele estar cifrado, mientras que el contenido sí⁸⁵¹. Ello se debe a la capacidad limitada de almacenamiento de Blockchain, pues este puede “identificar el archivo de forma unívoca y objetiva, proporcionando un resultado irrefutable. Prueba de su existencia y prueba de que se produjo la transferencia del bien”⁸⁵².

Encabezado	Carga Útil
○ Numero del bloque ○ El valor hash del encabezado del bloque anterior ○ Representación hash de los datos del bloque ○ Marca de tiempo ○ Tamaño del bloque ○ Nonce	○ Lista de transacciones ○ Otros tipos de datos

Tabla No 3. Datos almacenados en Blockchain. Fuente: elaboración propia.

Una transacción en Blockchain representa una interacción entre dos partes⁸⁵³, pero dependiendo del diseño de la cadena, se van aceptar determinados usos y almacenamiento. Por ejemplo, en las criptomonedas, una transacción suele transmitir la compraventa de activos digitales, pero también se puede emplear para enviar, tratar y almacenar datos (en el caso de los contratos inteligentes), o para registrar datos notariales, registros de propiedad, diplomas, o una obra creativa de propiedad intelectual, etc. Por la clase de información que suelen transmitir los datos contenidos en la carga útil, a estos datos se les conoce como datos transaccionales⁸⁵⁴. Dichos datos se pueden almacenar

⁸⁵⁰ YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain...*, Op. Cit., pp. 15-16.

⁸⁵¹ LI, Z. (2021). “Standardisation of Blockchain and Distributed Ledger Technologies—A Legal Voice from the Data Protection Law Perspective”, *25th EURAS Annual Standardisation Conference—Standards for Digital Transformation: Blockchain and Innovation (The European Academy for Standardisation)*, p. 4. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3892298 (fecha de consulta: 10 de septiembre de 2021).

⁸⁵² RAMPONE, F. (2018). “Data Protection...”, *cit.*, p. 9.

⁸⁵³ YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain...*, Op. Cit., p. 9.

⁸⁵⁴ GIANNPOULOU, A., & FERRARI, V. (2018). “Distributed data protection and liability on blockchains, *International Conference on Internet Science*, p. 5. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316954 (fecha de consulta: 28 de septiembre de 2021). Véase también EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, Op. Cit., p. 40.

como “texto sin formato, en forma cifrada o mediante *hash*”⁸⁵⁵, pero generalmente se almacena a través de las dos últimas herramientas⁸⁵⁶.

Tomando en consideración que, debido a las características de diseño de Blockchain, los datos almacenados en principio son inmutables, transparentes y públicos, cualquier persona con una conexión al sistema puede tener acceso a tales registros. Surge así, la pregunta de si un dato transaccional califica como dato personal bajo la legislación europea.

Para dar respuesta a esta pregunta es importante tener en cuenta el caso concreto, pues dependiendo del dato que se está transmitiendo, este puede considerarse o no un dato personal. Por ejemplo, una transacción de criptomonedas, donde una dirección A, le transmite cierta cantidad de dinero a una dirección B, en principio no calificaría como dato personal. No obstante, si esas direcciones se pueden vincular con una persona física, porque se pueden establecer sus identidades a través de plataformas de intercambios, si podrían calificar como tal.

Entonces, la cuestión aquí es si los datos personales que hagan referencia a una persona física identificada e identificable, a los cuales se les aplica la función *hash*, son datos anónimos, ya que la función *hash* no se considera por sí misma un dato personal, sino los datos que contiene. Para dar respuesta a este cuestionamiento primero analizaremos las opiniones del Grupo de Trabajo del artículo 29 y, luego, analizaremos una guía publicada por la Agencia Española de Protección de datos (AEPD) y el Supervisor Europeo de Protección De Datos (SEPD).

En 2007 en el Dictamen sobre el concepto de dato personal⁸⁵⁷, el Grupo de Trabajo afirmó que, con la utilización de criptografía unidireccional, como la función *hash*, se podían ocultar identidades sin dejar rastro alguno que permitiese vincular al seudónimo con una identidad, ya que en general esta función crea datos anónimos, es decir, que la función *hash* si podía anonimizar datos, debido a su unidireccionalidad, esto es, al hecho

⁸⁵⁵ Como quiera que la capacidad de almacenamiento de un bloque suele ser limitada y costosa por lo general la información se almacena como *hash*.

⁸⁵⁶ GIANNOPOULOU, A., & FERRARI, V. (2018). “Distributed...”, *cit.*, p. 4.

⁸⁵⁷ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007...*, *Op. Cit.*, p. 19.

de que no hay forma de obtener el conjunto de información original conociendo solamente el hash⁸⁵⁸. Posteriormente, en 2014 en el Dictamen sobre técnicas de anonimización⁸⁵⁹, el Grupo de Trabajo, con una postura absolutista de la anonimización, incluye al hash dentro de las técnicas de seudonimización, porque este es susceptible a ataques de fuerza bruta, lo que significa que la reidentificación del interesado, aunque difícil, es aún posible.

En 2019, bajo la vigencia del Reglamento General de Protección de datos, la AEPD y el SEPD emitieron una guía⁸⁶⁰ dirigida principalmente a los controladores que deseen implementar el hash para seudonimizar o anonimizar datos. Con un enfoque más matizado que el del Grupo de Trabajo del Artículo 29, el informe introduce la noción de riesgo de reidentificación en la utilización de las técnicas de hash y, además, establece la necesidad de realizar un análisis objetivo de ese riesgo para determinar si esas técnicas son adecuadas para seudonimizar o anonimizar⁸⁶¹.

La guía argumenta que, pese a que las funciones hash aspiran ser irreversibles, esto no impide que estén libres de riesgos, razón por lo cual hay que tenerlos en cuenta. Entre más información se tenga sobre los valores *hash*, las probabilidades de reidentificación aumentan. Para probar tal afirmación, ponen como ejemplo el tratamiento *hash* de número de teléfonos españoles, donde el número de caracteres y el prefijo son fijos (el prefijo es +34 y todo número móvil español empezará siempre por 6 o 7) y son conocidos con anterioridad, además que se puede saber el operador de cada número y el número aproximado de abonados totales españoles.

Con toda esta información se puede crear un diccionario para todos los *hashes* posibles de los teléfonos de una compañía de teléfono en menos de 20 segundos (la directriz menciona que un ordenador de sobremesa puede calcular más de 1 millón de *hashes* por segundo). Por otro lado, la existencia de identificadores adicionales (ya sean directos o indirectos) asociados al valor representado por el *hash*, hará que exista un

⁸⁵⁸ RAMPONE, F. (2018). “Data Protection...”, *cit.*, p. 9.

⁸⁵⁹ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014...*, *Op. Cit.* p.22.

⁸⁶⁰ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2019). *Introducción al hash como técnica de seudonimización de datos personales*. Disponible en: <https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf> (18) (fecha de consulta: 2 de octubre de 2021).

⁸⁶¹ La AEPD publica recomendaciones para aquellos que utilicen técnicas de hash en la seudonimización de datos.

mayor riesgo de identificar el contenido del mismo⁸⁶². Para impedir el riesgo de reidentificación, la directriz recomienda el empleo de estrategias para dificultar la reidentificación tales como: utilización de un algoritmo de cifrado con una clave que el controlador guarde de forma confidencial, agregar sal o ruido (agregar números aleatorios) al mensaje original.

Finalmente, la AEPD Y el SEPD exponen que los procesos de anonimización deben garantizar que incluso, el responsable del tratamiento no pueda reidentificar los datos anonimizados, por lo que, cuando este borra los elementos aleatorios introducidos o el ruido añadido, anonimiza los datos. En conclusión, la guía concluye que en ocasiones el *hash* puede anonimizar o seudonimizar datos, pero depende de una variedad de factores que varían desde las entidades involucradas hasta el tipo de datos en cuestión⁸⁶³.

Si bien el *hash* no es una técnica de anonimización per se, en ciertas circunstancias si puede llegar anonimizar datos personales⁸⁶⁴. Habrá que evaluar en cada caso concreto si el riesgo de reidentificación del dato personal que ha sido ofuscado a través de valores hash es razonablemente probable. Para ello, es necesario tener en cuenta los costes y el tiempo necesario para la identificación, así como la tecnología disponible en el momento del tratamiento, como los avances tecnológicos⁸⁶⁵ y la información disponible en manos de terceros.

Podemos concluir que, a menos que se apliquen técnicas adicionales, el *hash* no crea datos anónimos, por lo que, en Blockchain procesan datos personales, de modo que se aplica el Reglamento General de Protección de datos, aunque, el debate siga en curso en este sentido y no haya unanimidad por parte de la doctrina.

⁸⁶² AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2019). *Introducción al...*, Op. Cit. pp. 10-13.

⁸⁶³ GIANNOPOULOU, A. (2020). “Data Protection Compliance Challenges for Self-sovereign Identity”, *Congress on Blockchain and Applications*, p. 95. Disponible en: https://link.springer.com/chapter/10.1007%2F978-3-030-52535-4_10 (fecha de consulta: 23 de octubre de 2021).

⁸⁶⁴ Algunos autores que opinan en este sentido, véase: LI, Z. (2021). “Standardisation of Blockchain...”, *cit.*, p. 10 y RAMPONE, F. (2018). “Data Protection...”, *cit.*, p. 11.

⁸⁶⁵ Considerando 26 del RGPD.

2. Clave pública - criptografía asimétrica

En 1976, WHITFIELD DIFFE Y MARTY HELLMAN, criptógrafos de la Universidad de Stanford, sentaron las bases del concepto de criptografía de clave pública-privada, fundamento matemático para la seguridad de la computación y de la información de hoy en día⁸⁶⁶.

El cifrado de clave asimétrica, también conocido como criptografía de clave pública, es un método criptográfico que emplea una fórmula matemática para crear dos claves: una pública y una privada. Cada participante posee un par de claves, una pública y una privada. La clave privada debe mantenerse de forma confidencial, mientras que, la segunda es conocida y accesible para todos⁸⁶⁷. Ambas claves se mantienen unidas como una especie de llavero⁸⁶⁸, de tal forma que, la clave pública y privada del remitente cifran la información, mientras que la clave privada del receptor junto con la clave pública del remitente se emplea para el descifrado⁸⁶⁹. La clave privada es unidireccional, lo que significa que sirve para cifrar los datos, pero no para descifrarlo, pues solo la clave privada del destinatario puede hacerlo.

La criptografía de clave pública también proporciona la verificación de firmas digitales, la autenticación de los participantes y firmas digitales infalsificables⁸⁷⁰. Por ejemplo, María envía un mensaje secreto a Pedro utilizando su clave privada, de tal forma que la utilización de la clave privada de María le asegura a Pedro que el mensaje proviene de María. A su vez, Pedro solo puede descifrar el mensaje utilizando su clave privada, que solo él conoce. Véase gráfico No. 5.

⁸⁶⁶ ANTONOPOULOS, A. (2017). *Mastering Bitcoin Programming the Open Blockchain*, O'Reilly Media, Inc, p. 56.

⁸⁶⁷ SINGHAL, B., DHAMEJA, G. & SEKHAR PANDA, P. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*, Apress, New York, p. 80. Disponible en: https://link.springer.com/chapter/10.1007/978-1-4842-3444-0_2#Sec2 (fecha de consulta: 1 de marzo de 2022).

⁸⁶⁸ “Cifrado asimétrico”. (2022). Disponible en: <https://www.ionos.es/digitalguide/servidores/seguridad/cifrado-asimetrico/> (fecha de consulta: 20 de mayo de 2022).

⁸⁶⁹ VAN DER AUWERA E., SCHOUTENS W., PETRACCO GIUDICI M. & ALESSI L. (2020) “Blockchain”, *Financial Risk Management for Cryptocurrencies*. (Drs. VAN DER AUWERA E., SCHOUTENS W., PETRACCO GIUDICI M. & ALESSI L.), Ed.: Springer, Cham. p. 7.

⁸⁷⁰ ANTONOPOULOS, A. (2017). *Mastering..., Op. Cit.*, p. 56.

En conclusión, las claves públicas se emplean para cifrar la información o para verificar las firmas. Las claves privadas se utilizan para descifrar la información o para crear firmas⁸⁷¹.



Figura No. 5. Fuente: elaboración propia. Gráfico hecho con iconos realizados en www.flaticon.com

2.1 Criptografía asimétrica en Blockchain

Normalmente en una cadena de bloques los nodos no revelan su identidad real, sino que suelen interactuar con la red a través un identificador público compuesto por una serie de caracteres alfanuméricos de aspecto aleatorio⁸⁷², esto es, una clave pública. Dicha clave es una dirección que funciona como una especie de número de cuenta bancaria que está vinculada a la clave privada (que a su vez hace las veces de una contraseña). Con la diferencia de que, tratándose de una Blockchain pública, los usuarios pueden crear tantas claves como a bien tengan.

En la mayoría de las implementaciones Blockchain, la criptografía asimétrica hace posible la confianza entre desconocidos, ya que permite verificar las firmas digitales y autenticar a los participantes. La clave pública o dirección es empleada como punto final de entrada y salida en una transacción⁸⁷³, es decir, permite a los participantes enviar y recibir dinero. Por ejemplo, en una Blockchain de criptomonedas, supongamos Bitcoin, María le envía 1 *BTC* a Pedro. María firma y aprueba la transacción utilizando su clave

⁸⁷¹ SINGHAL, B., DHAMEJA, G. & SEKHAR PANDA, P. (2018). *Beginning Blockchain: A Beginner's Guide ...*, Op. Cit., p. 80.

⁸⁷² CNIL. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*, p. 6. Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf (fecha de consulta: 9 de octubre de 2021).

⁸⁷³ YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain...*, Op. Cit., p. 13

privada. Luego, la transacción es transmitida a todos los nodos de la cadena de bloques⁸⁷⁴ y si se comprueba la disponibilidad de los fondos, esta se valida. Posteriormente, se actualizan los saldos de las cuentas⁸⁷⁵ y la transacción se añade dentro de un bloque. Pedro, a su vez, puede gastar los fondos enviados a su clave pública, autorizando con su clave privada y repitiendo el mismo proceso.

Asimismo, la criptografía asimétrica puede ser empleada no solo para crear direcciones públicas de los participantes, sino que también funciona como un modo de acceso a los Smart Contracts, una vez que estos se han implementado dentro de la red Blockchain⁸⁷⁶. Por ejemplo, en Ethereum los contratos inteligentes son un tipo de cuenta de Ethereum, es decir, son un tipo de dirección que, al igual que las cuentas de propiedad externa, el otro tipo de cuenta de esta red, pueden recibir, enviar y almacenar *ETH* y token e interactuar con otros Smart Contracts⁸⁷⁷.

2.2 ¿Las claves públicas son datos personales?

Cuando un nodo firma con su clave privada una transacción, esta es transmitida por toda la red, por lo que es visible por todos. No obstante, el resto de participantes no saben quién está detrás de esa dirección, porque lo que ven es una dirección (la clave pública). Es decir, el usuario se identifica de forma indirecta. Sin embargo, los datos transaccionales son públicos y transparentes. Una red Blockchain en principio podría preservar la privacidad de esta forma, pero surge la cuestión de si la clave pública como se usa comúnmente en una cadena de bloques constituye un dato de carácter personal o si, por el contrario, es suficiente para anonimizar a los usuarios.

La respuesta a este planteamiento por parte de la doctrina es casi unánime. La clave pública pertenece a la categoría de datos seudónimos y, por tanto, constituye procesamiento de datos personales, por lo que está bajo el ámbito de aplicación del Reglamento General de Protección de Datos. Algunos autores que argumentan en este

⁸⁷⁴ ZHENG, Z., XIE, S., DAI, H., CHEN, X., & WANG, H. (2017). "An overview of blockchain technology: Architecture, consensus, and future trends", *IEEE international congress on big data (BigData congress)*. Disponible en: <https://ieeexplore.ieee.org/document/8029379> (fecha de consulta: 1 de noviembre de 2021).

⁸⁷⁵ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 21.

⁸⁷⁶ YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain...*, Op. Cit., pp. 13.

⁸⁷⁷ "Cuentas de Ethereum" (2022). Disponible en: <https://ethereum.org/es/developers/docs/accounts/> (fecha de consulta: 1 de abril de 2022).

sentido son: MANTEGHI⁸⁷⁸, DE FILIPPI⁸⁷⁹, BUOCZ y otros⁸⁸⁰, GIANNOPOULOU⁸⁸¹, TEPERDJIAN⁸⁸², FINCK⁸⁸³, así como el Parlamento Europeo⁸⁸⁴, la Agencia Española de Protección de Datos⁸⁸⁵, la Agencia de Protección de Datos Francesa (CNIL, por sus siglas en francés, *Commission Nationale Informatique & Libertés*) y El Observatorio Y Foro De Blockchain De La Unión Europea⁸⁸⁶. Ello se debe porque las claves públicas, al ser combinada con otro tipo de datos, pueden revelar la identidad de los participantes. La mayoría de las veces, esta información está disponible públicamente y son los mismos usuarios quienes proporcionan sus direcciones en redes sociales. Lo hacen ya sea para la recepción de criptomonedas o para demostrar que son miembros de una comunidad. Sin embargo, con estas acciones no solo revelan sus claves públicas, sino que también desvelan información personal como el sexo, la edad, la ubicación, entre otras⁸⁸⁷. Asimismo, la legislación contra el blanqueo de capitales o *Anti-Money Laundering* (AML) y el cumplimiento de las normas de KYC (por sus siglas en inglés, *Know your Customer* o Conoce a tu cliente, en español), hace que los sitios de intercambios de criptomonedas, billeteras y servicios de pagos con criptomonedas recaben información personal de sus clientes. Es importante aclarar que, para que un usuario de criptomonedas, no dependa de ningún intermediario, es decir, de una plataforma de intercambio y de una *wallet* (billetera) para gestionar, administrar, comprar o enviar criptomonedas este debe instalar un nodo completo (que supone descargar una copia completa de la

⁸⁷⁸ MANTEGHI, M. (2021). “Blockchain and...”, *cit.*, p. 11.

⁸⁷⁹ DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, *Op. Cit.*, p. 38 y DE FILIPPI, P. (2016). “The interplay between decentralization and privacy: the case of blockchain technologies”, *Journal of Peer Production*, No.7, p. 11. Disponible en: <https://hal.archives-ouvertes.fr/hal-01382006/document> (fecha de consulta: 7 de diciembre de 2021).

⁸⁸⁰ BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). “Bitcoin and the GDPR: allocating responsibility in distributed networks”, *Computer Law & Security Review*, Vol. 35, No. 2, p. 186. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0267364918303170> (fecha de consulta: 2 de enero de 2022).

⁸⁸¹ GIANNOPOULOU, A., & FERRARI, V. (2018). “Distributed data...”, *cit.*, p. 5.

⁸⁸² TEPERDJIAN, R. (2020). “The Puzzle...”, *cit.*, p. 27.

⁸⁸³ FINCK, M. (2017). “Blockchains and Data Protection in the European Union”, *Max Planck Institute for Innovation & Competition Research*, Paper 18-01, p. 1. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (fecha de consulta: 17 de enero de 2022).

⁸⁸⁴ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain and...*, *Op. cit.*, p. 26.

⁸⁸⁵ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021). “Cifrado y Privacidad (V): la clave como dato personal”. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-la-clave-como-dato-personal> (fecha de consulta: 20 de enero de 2022).

⁸⁸⁶ EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FÓRUM. (2018). *Blockchain An...*, *Op. Cit.*, p. 20.

⁸⁸⁷ AL JAWAHERI, H., AL SABAH, M., BOSHMAF, Y., & ERBAD, A. (2020). “Deanonymizing Tor hidden service users through Bitcoin transactions analysis”, *Computers & Security*, Vol. 8. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404818309908> (fecha de consulta: 17 de enero de 2022).

Blockchain). Por ejemplo, en Bitcoin, entre los requisitos para convertirse en un nodo completo encontramos, 350 GB de espacio en disco, 2 GB de memoria RAM, una conexión a internet de banda ancha de al menos 400 *kilobits* por segundo, 6 horas de actividad al día, entre otros⁸⁸⁸. Estos requerimientos se vuelven tediosos para muchos usuarios, de modo que, por eso muchos optan por emplear intermediarios, es más, a la fecha de 7 de octubre de 2022, 15652 nodos completos en todo el mundo⁸⁸⁹, de los cuales hay 64 en España. No obstante, si un usuario necesita intercambiar sus criptomonedas por dinero Fiat y viceversa (a menos que sea un minero y extraiga sus propias criptomonedas), necesariamente tendrá que emplear un intermediario, puesto que, mediante el *software* de la cadena no se puede realizar.

El historial de transacciones es visible por todos, porque la transparencia constituye uno de los ejes centrales de esta tecnología, de ahí que la posibilidad de reidentificación aumente cuando se reutilizan las claves públicas⁸⁹⁰, pues se incrementa el riesgo de vinculación debido a que empiezan a surgir patrones de uso⁸⁹¹, lo que plantea serias preocupaciones con respecto a la privacidad de los usuarios. De hecho, varias heurísticas han demostrado que es posible desanonimizar a los usuarios. Por ejemplo, un estudio⁸⁹² llevado a cabo por investigadores de la Universidad de Luxemburgo presentó un método que permite vincular los seudónimos de los usuarios con las direcciones IP donde se generan las transacciones, aun cuando los usuarios utilizan traducción de direcciones de red⁸⁹³, cortafuegos de sus ISPs (Proveedor de servicios de internet) o cuando usan servicios de anonimato como TOR (*The Onion Router*, en inglés). Así como individualizar a los nodos dentro de una misma dirección IP.

⁸⁸⁸ “Running A Full Node” (Sin fecha). Disponible en: <https://bitcoin.org/en/full-node#what-is-a-full-node> (fecha de consulta: 7 de octubre de 2022).

⁸⁸⁹ La estimación es de nodos alcanzables. El tamaño estimado con nodos inalcanzables es de: 41354 consulte: <https://bitnodes.io/> (fecha de consulta: 7 de octubre de 2022).

⁸⁹⁰ MANTEGHI, M. (2021). “Blockchain and...”, *cit.*, p.10.

⁸⁹¹ Véase HERRERA, F. (Sin fecha). “Blockchain, anonimización y Reglamento General de Protección de Datos”. Disponible en: <https://blog.sepin.es/2019/04/blockchain-anonimizacion-rgpd/> (fecha de consulta: 23 de enero de 2022) y EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. (2018). *Blockchain An..., Op. Cit.*, p. 20.

⁸⁹² BIRYUKOV, A., KHOVRATOVICH, D. & PUSTOGAROV, I. (2014), “Deanonymisation of clients in Bitcoin P2P network”, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. Disponible en: <https://dl.acm.org/doi/10.1145/2660267.2660379> (fecha de consulta: 23 de enero de 2022).

⁸⁹³ Comúnmente conocido por el acrónimo NAT que significa Network Address Translation, (traducción de direcciones de red) o enmascaramiento de direcciones IP.

De igual forma, otro estudio realizado por investigadores de la Universidad de California y de la Universidad George Mason emplearon un sistema conocido como análisis de gráficos de transacciones, con el cual “lograron identificar grupos de comerciantes y clientes que confiaban en la cadena de bloques de Bitcoin”⁸⁹⁴. Asimismo, otro estudio llevado a cabo en 2019 desanonimizó a usuarios de Tor mediante el análisis de transacciones de Bitcoin. En esta misma línea, una investigación del año 2015 demostró que los clientes que usan Bitcoin por intermedio de TOR obtienen un nivel limitado de anonimato y son vulnerables a los ataques de intermediarios⁸⁹⁵, pues el atacante puede tomar sus huellas digitales, reconocerlos y aprender sus direcciones IP e identificarlos ⁸⁹⁶.

Igualmente, una investigación de 2020 demostró que el empleo de Bitcoin como medio de pago en los servicios ocultos de Tor, filtra información que puede usarse para desanonimizar sus usuarios y puede revelar información confidencial como la ubicación, edad, sexo, direcciones de correo electrónico. A través del análisis de transacciones de Bitcoin, un tercero puede vincular retroactivamente a los nodos, que comparten públicamente sus claves públicas en las redes sociales, con los servicios ocultos que comparten públicamente sus direcciones de Bitcoin en sus páginas de destino. Por ejemplo, vincular usuarios de Twitter con servicios ocultos como Silk Road⁸⁹⁷. Es conveniente traer a colación otro proyecto llevado a cabo por investigadores del *College of Information Sciences and Technology* y la universidad estatal de Pensilvania, que logró obtener información sobre la ubicación física y los hábitos de consumos de los usuarios

⁸⁹⁴ MEIKLEJOHN, S., POMAROLE, M., JORDAN, G., LEVCHENKO, K., MCCOY, D., VOELKER, G. M., & SAVAGE, S. (2013). “A fistful of bitcoins: characterizing payments among men with no names”, *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127-140. Disponible en: <https://dl.acm.org/doi/10.1145/2896384>, Como se citó en DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain...*, Op. Cit., p. 39.

⁸⁹⁵ Un ataque de intermediario (man-in-the-middle, MITM) es un ataque a través del cual un tercero intercepta una comunicación entre usuarios (o máquinas), es decir que el atacante se coloca entre la persona y la actividad que se esté realizando en línea, por ejemplo, entre el banco y un usuario. Véase “Ataques de intermediarios “¿Qué son, y cómo podemos evitarlos?” (Sin fecha). Disponible en: https://www.internetsociety.org/wp-content/uploads/2020/12/Man-in-the-Middle-Fact-Sheet_final_ES.pdf (fecha de consulta: 22 de marzo de 2022).

⁸⁹⁶ BIRYUKOV, A. & PUSTOGAROV, I. (2015). “Bitcoin over Tor isn't a Good Idea,” *2015 IEEE Symposium on Security and Privacy*. Disponible en: <https://ieeexplore.ieee.org/document/7163022> (fecha de consulta: 21 de marzo de 2022).

⁸⁹⁷ JAWAHERI, H., AL SABAH, M., BOSHMAF, Y., & ERBAD, A. (2020). “Deanonymizing Tor hidden service users through Bitcoin transactions analysis”, *Computers & Security*, Vol. 89. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404818309908#bib0013> (fecha de consulta: 21 de marzo de 2022).

de Bitcoin⁸⁹⁸. Una investigación más reciente, a través del empleo de fuentes públicas, logró vincular las direcciones de Bitcoin con entidades reales⁸⁹⁹.

Hemos podido observar que el 100% de estos estudios hacen referencia a Bitcoin, ya que es la Blockchain más popular y la que más atención recibe, no obstante, la desanonimización no se da solo en el contexto Bitcoin, sino que también podemos encontrar estudios que demuestran que los usuarios de Ethereum también son susceptibles de ser identificados. En particular, un trabajo de 2021 propuso un enfoque para desanonimizar las transacciones mediante la vinculación de las direcciones que se emplearon para implementar contratos inteligentes, que fueron redactados por las mismas personas. Mediante la estilometría, una técnica que se usa en las ciencias sociales para atribuir la autoría de textos literarios. Los investigadores hicieron una analogía entre el texto literario y el código fuente de los Smart Contracts para examinar hasta qué punto las características únicas del código fuente y el código de bytes de dichos contratos puede representar el estilo de codificación de los desarrolladores. El estudio demostró que incluso un pequeño número de rasgos representativo conduce a una precisión suficientemente alta en la atribución del código de los contratos inteligentes a la dirección de su autor⁹⁰⁰.

Otro estudio del año 2021, eliminó del anonimato a clientes de Ethereum empleando el Servicio De Nombres Ethereum (ENS, por sus siglas en inglés, *Ethereum Name Service*)⁹⁰¹ y aplicando técnicas de aprendizaje automático al gráfico de transacciones de Ethereum, para vincular las direcciones que pertenecen al mismo dueño, así como técnicas de creación de perfiles de usuario basadas en la actividad de la hora del día y la tarifa de transacción⁹⁰² para desanonimizar a los participantes. Otra investigación

⁸⁹⁸ DUPONT, J., & SQUICCIARINI, A. C. (2015, March). "Toward de-anonymizing bitcoin by mapping users location", *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. Disponible en: <https://dl.acm.org/doi/10.1145/2699026.2699128> (fecha de consulta: 25 de marzo de 2022).

⁸⁹⁹ MAKAROV, I., & SCHOAR, A. (2022). "Blockchain analysis of the bitcoin market". Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3942181 (fecha de consulta: 26 de marzo de 2022).

⁹⁰⁰ LINOY, S., STAKHANOVA, N., & RAY, S. (2021). "De-anonymizing Ethereum blockchain smart contracts through code attribution. *International Journal of Network Management*", Vol. 31, No 1. Disponible en <https://doi.org/10.1002/nem.2130> (fecha de consulta: 26 de marzo de 2022).

⁹⁰¹ Es un servicio que funciona parecido al sistema de nombres de dominio de internet. Se trata de una función que ayuda a los usuarios asignar nombres legibles y fáciles de recordar a las direcciones (claves públicas) de Ethereum, en lugar de una secuencia larga alfanumérica.

⁹⁰² BÉRES, F., SERES, I. A., BENCZÚR, A. A., & QUINTYNE-COLLINS, M. (2021). "Blockchain is watching you: Profiling and deanonymizing ethereum users", *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Disponible en: <https://arxiv.org/abs/2005.14051> (fecha de consulta: 26 de marzo de 2022).

de 2021 evidenció que el anonimato de la red Ethereum es limitado. Los autores se basaron en el análisis de redes *peer-to-peer*, y observaron que, mediante mediciones y análisis, un atacante puede establecer conexiones con aproximadamente el 90% de los nodos completos sincronizados de Ethereum y eliminar del anonimato a los participantes de una transacción⁹⁰³.

Hay que mencionar, además, que existen compañías que se dedican profesionalmente al análisis forense de las cadenas de bloques a gran escala, y cuyo trabajo consiste en eliminar del anonimato a los usuarios. Proveedores como, Chainalysis⁹⁰⁴, CipherTrace⁹⁰⁵, Merkle Science⁹⁰⁶ y Elliptic⁹⁰⁷, trabajan con agencias gubernamentales, fuerzas de seguridad, reguladores e instituciones financieras para investigar delitos relacionados con la criptoconomía. De esta lista se destaca Chainalysis, que se ha convertido en el principal contratista de análisis criptográfico de los Estados Unidos. En este sentido, la desanonimización de las identidades en una cadena de bloques ya no queda limitada a la investigación académica, sino que es una industria en crecimiento, que puede estar al alcance de cualquier persona.

En consecuencia, no queda duda que las claves públicas califican como datos personales⁹⁰⁸ y, más específicamente, como datos seudónimos, pues hacen parte de la identidad del usuario⁹⁰⁹. El RGPD establece que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente, en particular mediante un identificador en línea, de tal forma que las claves públicas entran en la categoría de identificadores en línea de que trata el considerando 30 del Reglamento General de Protección de datos⁹¹⁰. Como acertadamente señala la AEPD, “la clave pública es un

⁹⁰³GAO, Y., SHI, J., WANG, X., SHI, R., YIN, Z., & YANG, Y. (2021). “Practical Deanonymization Attack in Ethereum Based on P2P Network Analysis”, *IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*. Disponible en: <https://ieeexplore.ieee.org/document/9644904/references#references> (fecha de consulta: 26 de marzo de 2022).

⁹⁰⁴ “Chainalysis”. (Sin fecha). <https://www.chainalysis.com/> (fecha de consulta: 1 de abril de 2022).

⁹⁰⁵ “Ciphertrace”. (Sin fecha). Disponible en: <https://ciphertrace.com/> (fecha de consulta: 1 de abril de 2022).

⁹⁰⁶ “Merklescience”. (Sin fecha). Disponible en: <https://www.merklescience.com/> (fecha de consulta: 1 de abril de 2022).

⁹⁰⁷ “Elliptic”. (Sin fecha). Disponible en: <https://www.elliptic.co/> (fecha de consulta: 1 de abril de 2022).

⁹⁰⁸ Lógicamente, si quien está detrás es una persona física, porque si es una persona jurídica o algún tipo de organización no tendría tal calificación.

⁹⁰⁹ GIANNOPOULOU, A. (2020). “Data Protection...”, *cit.*, p. 80.

⁹¹⁰ “Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de

identificador unívoco por su propia naturaleza, pues la probabilidad de que dos personas puedan compartir la cadena de caracteres que constituyen una clave es prácticamente nula”⁹¹¹. Es más, la clave pública está asociada a otros identificadores únicos como son las cookies, direcciones IP, firmas de dispositivo, entre otros, que son considerados datos personales. Todos estos identificadores, si son analizados con información adicional, tienen la capacidad de perfilar a los usuarios, singularizarlos e identificarlos.

Esto se entiende mejor con la sentencia de Breyer contra Bundesrepublik Deutschland⁹¹², referente a las direcciones IP dinámicas⁹¹³, una dirección que cambia cada vez que se establece una nueva conexión a internet⁹¹⁴. En este asunto, el TJUE analizó el concepto de identificabilidad indirecta de los interesados⁹¹⁵. Con el objetivo de evitar ataques informáticos y posibilitar el ejercicio de acciones penales contra los piratas, los sitios web de organismos federales alemanes registraban y almacenaban las direcciones IP dinámicas y otros datos de los usuarios que accedían a estas páginas. No obstante, solo el Proveedor de Servicios de internet contaba con información adicional que permitía identificar a un abonado, mientras que, la República Federal de Alemania, en su calidad de proveedor de servicios de medios en línea (quien almacenaba las direcciones IP) no contaba con información adicional para identificar a un usuario. El TJUE consideró que las direcciones IP dinámicas recopiladas por un proveedor de servicios de medios en línea constituye datos personales, solo cuando este dispone de medios legales que le permitan identificar a un usuario gracias a la información adicional de que dispone el proveedor de servicios de internet de ese usuario. El proveedor de servicios de medios en línea dispone de medios razonables para identificar al interesado,

«cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas”.

⁹¹¹ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021). “Cifrado y...”, *cit*.

⁹¹² STJUE, Sala 2ª, de 19 de octubre de 2016, apartado 43. Si bien esta sentencia es anterior al RGPD, recordemos que la definición de datos personales de la Directiva y el reglamento son materialmente similares, por lo que sigue siendo relevante bajo la vigencia del RGPD.

⁹¹³ Según STJUE, Sala 2ª, de 19 de octubre de 2016, apartado 16 “a diferencia de las direcciones IP estáticas, las direcciones IP dinámicas no permiten relacionar, mediante ficheros accesibles al público, un ordenador concreto y la conexión física a la red utilizada por el proveedor de acceso a Internet”.

⁹¹⁴ Recordemos que, en STJUE, Sala 3ª, de 24 de noviembre de 2011, Asto: C-70/10, Scarlet Extended SA/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-70/10&td=ALL> (fecha de consulta 10 de abril de 2022) el TJUE ya había considerado que las direcciones IP estáticas constituían datos personales “son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios”.

⁹¹⁵ AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2018). *Manual...*, Op. Cit., p. 105.

con la ayuda de terceros, en este caso, la autoridad competente y el proveedor de servicios de internet, a partir de las direcciones IP que almacena. Por tanto, la información que esté en manos de un tercero constituye un medio que puede ser razonablemente utilizado, a menos que, como lo indica el abogado General, implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos y el riesgo de identificación parece en realidad ser insignificante o esté prohibido por la ley. En tal caso, no constituiría un medio razonable. Como advierte FINK, esta situación es en muchos aspectos análoga a las plataformas de intercambios de criptomonedas u otros proveedores que están legalmente obligados a recopilar datos, en virtud de lo establecido en las normas de prevención del blanqueo de capitales y KYC⁹¹⁶.

Algunos desarrollos Blockchain como ZCASH⁹¹⁷ y MONERO⁹¹⁸ apuntan a la privacidad de sus usuarios, son capaces de ocultar las direcciones, el monto y el rastro de las transacciones, así como la identidad del remitente y el receptor⁹¹⁹. Monero es una criptomoneda lanzada en el año 2014, anónima por defecto. El remitente, el receptor y el importe de cada transacción se ocultan mediante el uso de tres importantes tecnologías:

- i. *Direcciones ocultas*: Permite mantener oculta la dirección del receptor. Una dirección oculta es una dirección de un solo uso para cada transacción. Si un tercero observa Monero no puede vincular la dirección publicada del destinatario ni a las direcciones de ninguna otra transacción. Es decir, que, si A le envía dinero a B, la salida recibida por B no se asocia con la dirección del monedero de B⁹²⁰.

⁹¹⁶ FINCK, M. (2017). “Blockchains and...”, *cit.*, p. 14.

⁹¹⁷ “Zcash”. (Sin fecha). Disponible en: <https://z.cash/> (fecha de consulta: 10 de mayo de 2022).

⁹¹⁸ “Monero” (Sin fecha). Disponible en: <https://www.getmonero.org/> (fecha de consulta: 10 de mayo de 2022).

⁹¹⁹ CHANDRASEKERA, S. (2020). “IRS Is Trying To Deanonymize Privacy Coins Like Monero And Zcash”. Disponible en: <https://www.forbes.com/sites/shehanchandrasekera/2020/07/06/irs-is-trying-to-deanonymize-privacy-coins-like-monero-and-zcash/?sh=433ce9374174> (fecha de consulta: 10 de mayo de 2022).

⁹²⁰ Véase: “Stealth addresses” (Sin fecha). Disponible en: <https://www.getmonero.org/es/resources/moneropedia/stealthaddress.html> (fecha de consulta: 17 de abril de 2022). “Stealth Addresses – Que es y por qué la utiliza Monero?” (2022). Disponible en: <https://satoshirov.com/stealth-addresses-que-es-y-por-que-la-utiliza-monero/> (fecha de consulta: 10 de mayo de 2022).

ii. *Firmas de anillo*: Las firmas de anillo es un tipo de firma digital que hace posible que se pueda ocultar la dirección del remitente mezclando la firma de este con un grupo de otras direcciones⁹²¹.

iii. *RingCT*: es la abreviatura de *Ring Confidential Transactions*, es un tipo de firma de anillos, introducido en esta plataforma en 2017, es la tecnología que oculta el valor de los fondos de las transacciones⁹²². Solo las partes involucradas en la transacción pueden ver el monto que se transfiere.

Las transacciones no pueden ser rastreadas, por lo que no es transparente, sino opaca. En contraste con Monero, Zcash no es una criptomoneda de privacidad por defecto, sino que son los usuarios quienes deciden si sus transacciones son anónimas o no. Zcash permite que el remitente, el destinatario y la cantidad de dinero estén encriptados y sean completamente privados gracias a la utilización de un protocolo criptográfico llamado prueba conocimiento cero (*Zero-knowledge proof*), el cual permite verificar una transacción sin necesidad de conocer los datos de la misma.

Hasta el momento, estas soluciones de privacidad, han sido bastante efectivas para mantener el anonimato a sus participantes. De hecho, en 2020 La División de Investigación Criminal (CID) del Servicio de Impuestos Internos (IRS) de los Estados Unidos contrató a la empresa de análisis forense Chainalysis, para estudiar y analizar los protocolos de seguridad de tales Blockchain que ayuden a eliminar del anonimato a sus participantes, ya que su uso ha venido en aumento y ha sido relacionado con actividades ilícitas⁹²³.

Como quiera que debemos tener en cuenta la tecnología disponible y los avances tecnológicos, es posible que estas implementaciones dejen de ser anónimas, habida cuenta

⁹²¹ Véase: “Ring signature” (Sin fecha). Disponible en: <https://www.getmonero.org/es/resources/moneropedia/ringsignatures.html> (fecha de consulta: 15 de abril de 2022). “¿Qué son Las firmas de anillo?”. (2021). Disponible en: <https://crypto4dummy.com/que-son-las-firmas-de-anillo/> (fecha de consulta: 10 de mayo de 2022).

⁹²² RingCT, es la abreviatura de Ring Confidential Transactions, es la tecnología que oculta los montos de las transacciones. Véase “Ring CT” (Sin fecha) Disponible en: <https://www.getmonero.org/resources/moneropedia/ringCT.html> fecha de consulta: 12 de mayo de 2022).

⁹²³ LI, S. (2020) “IRS Hoping to Deanonymize Monero and ZCash Privacy Coins to Prevent Cybercrime”. Disponible en: <https://blockchain.news/news/irs-hoping-deanonymize-monero-zcash-privacy-coins-prevent-cybercrime> (fecha de consulta: 23 de mayo de 2022).

de que los datos se registran de forma permanente en las cadenas de bloques. Entonces, podemos concluir que, cuando las claves públicas están relacionadas con una persona física, se consideran como datos seudónimos, pues al ser combinada con información adicional permiten la identificación del interesado. En última instancia, las cadenas de bloques no garantizan la privacidad de sus usuarios, como se hizo creer en un principio, es más, “la mayoría de las transacciones de criptomonedas han resultado ser menos privadas que la banca tradicional, pues esta está sometida a regulaciones gubernamentales que le exigen unas protecciones básicas de privacidad”⁹²⁴. Las cadenas de bloques son un registro público de las transacciones que en ella se ejecutan, si alguien conoce la clave publica de alguien, puede rastrear todos sus movimientos y conocer su actividad monetaria.

III.DESAFÍOS DE LOS DERECHOS DE LOS INTERESADOS

El RGPD le confiere al interesado distintos derechos que le permiten intervenir en las labores de tratamiento llevadas a cabo por el responsable y el encargado. Uno de los objetivos del Reglamento es empoderar a las personas y darles el control sobre sus datos, no obstante, la inmutabilidad y descentralización de Blockchain suponen un problema potencial en el ejercicio de estos derechos, ya que, en principio, la información almacenada en Blockchain no se puede eliminar o modificar. Asimismo, la red es distribuida y no hay un punto o autoridad central, lo que dificulta la identificación del responsable del tratamiento, sujeto responsable de la aplicabilidad de estos derechos, quien es el encargado de atender las solicitudes.

Los derechos de los interesados, como supresión y rectificación, suponen la posibilidad de modificar o eliminar los datos, lo que, lógicamente, va en contravía con la inmutabilidad de las cadenas de bloques, ya que estas son un enlace de bloques posteriores y un solo bloque corrupto afectará a toda la equivalencia⁹²⁵.

⁹²⁴ HENRY, R., HERZBERG, A., & KATE, A (2018). "Blockchain Access Privacy: Challenges and Directions", *IEEE Security & Privacy*, vol. 16, No. 4, pp. 38-45. Disponible en: <https://ieeexplore.ieee.org/document/8425613> (fecha de consulta: 2 de mayo de 2022)

⁹²⁵ MEIJER, C. R. (2018). "Blockchain versus GDPR and who should adjust most". Disponible en: <https://www.finextra.com/blogposting/16102/blockchain-> (fecha de consulta: 1 de abril de 2022).

No obstante, es importante advertir que como hemos venido mencionando, existen diferentes modelos de Blockchain, por lo que la capacidad de cumplir con tales derechos difiere, según el diseño de la plataforma⁹²⁶. Esto debe verse con diferentes matices, pues hay Blockchains diseñadas específicamente para proteger la privacidad⁹²⁷, como la cadena de bloques de carácter privada MyHealthMyData⁹²⁸, aunque el cumplimiento de las leyes de privacidad por parte de esta, no ha sido discutido por ninguna autoridad legal.

Por consiguiente, a simple vista pareciese que debido al diseño del RGPD, elaborado para un mundo centralizado, que contempla el procesamiento de datos solo en una dimensión vertical en cabeza del responsable del tratamiento⁹²⁹, fuese completamente incompatible en el contexto de las cadenas de bloques descentralizadas y públicas, no solo a nivel técnico, sino también a nivel conceptual⁹³⁰. En consecuencia, en esta sección abordaremos los derechos del titular amparados por el Reglamento que a simple vista entran en conflicto con Blockchain, pero nos centraremos en el estudio de las cadenas de bloques de carácter públicas, las cuales por su naturaleza abierta y distribuida suponen un verdadero reto.

1. Derecho al olvido en Blockchain

Resulta complejo conciliar el borrado de datos en una tecnología que tiene como ejes fundamentales su capacidad de inalterabilidad y descentralización. Intencionalmente, el diseño de una cadena de bloques hace que sea prohibitivamente costoso eliminar o modificar la información, ya que su objetivo es crear confianza y asegurar la integridad de la red⁹³¹.

⁹²⁶ BACON, J., MICHELS, J. D., MILLARD, C., & SINGH, J. (2018). “Blockchain demystified ...”, *cit.*, p. 76.

⁹²⁷ RAMPONE, F. (2018). “Data Protection...”, *cit.*, p. 4.

⁹²⁸ Véase BAYLE, A., KOSCINA, M., MANSET, D., & PEREZ-KEMPNER, O. (2018). “When blockchain meets the right to be forgotten: technology versus law in the healthcare industry”, *IEEE/WIC/ACM International Conference on Web Intelligence*, pp. y ss. Disponible en: <http://www.myhealthmydata.eu/wp-content/uploads/2019/10/When-Blockchain-Meets-the-Right-to-be-Forgotten.pdf> (fecha de consulta: 9 de junio de 2022).

⁹²⁹ Data Protection in the Blockchain Environment GDPR is not a Hurdle to Permissionless DLT Solutions p. 2

⁹³⁰ GDPR Vs. Blockchain – Technology Against The Law (Sin fecha). Disponible en: <https://www.eurolatamlex.com/publications/news/42-gdpr-vs-blockchain-technology-against-the-law.html> (fecha de consulta: 2 de mayo de 2022).

⁹³¹ LI, Z. (2021). “Standardisation of Blockchain...”, *cit.*, p. 6.

En este apartado, intentaremos dar respuesta a la pregunta ¿es compatible el derecho al olvido con Blockchain? Para resolver este interrogante y teniendo en cuenta los diferentes diseños de Blockchain, nos enfocaremos en cadenas de bloques abiertas y públicas (como puede ser Bitcoin o Ethereum), que implican un desafío mayor en la aplicación del derecho al olvido, pues en una cadena de bloques privada están en mejor posición para cumplir con el derecho de supresión, pues (por ejemplo, Hyperledger⁹³² o Corda⁹³³) dependen de una autoridad central y jerárquica que determina las reglas sobre la misma, y a su vez, puede incorporar en su arquitectura, técnicas que permitan el borrado de datos, así como establecer reglas de consenso para modificar la información almacenada dentro de la red. Evidentemente, la identificación del responsable y del encargado del tratamiento no suponen un problema para este tipo de Blockchains, ya que su identidad se puede determinar de forma clara. Y tal como hemos mencionado, la identificación de estos sujetos es necesaria, pues ante quien debe acudir el interesado para reclamar el ejercicio de sus derechos.

El desarrollo de esta sección está estructurado de la siguiente manera, primero analizaremos qué es el derecho al olvido a la luz del RGPD, a continuación, analizaremos lo que significa la supresión, y finalmente abordaremos las distintas soluciones técnicas que han surgido para dar cumplimiento a lo estipulado en el artículo 17.

1.1 Derecho de supresión (el derecho al olvido)

Señala la AEPD que el derecho al olvido “es la manifestación del derecho de supresión aplicado a los buscadores de internet”⁹³⁴. Reconocido por el TJUE en el caso Google España, el derecho al olvido se sustenta en el derecho de supresión establecido en el artículo 17 de del RGPD⁹³⁵ que señala que, el interesado tiene derecho a que se supriman los datos que le concierne sin dilaciones indebidas y describe seis circunstancias

⁹³² Véase “hyperledger”. (Sin fecha). Disponible en: <https://www.hyperledger.org/> (fecha de consulta: 10 de mayo de 2021).

⁹³³ Véase “Corda”. (Sin fecha). Disponible en: <https://corda.net/> (fecha de consulta: 10 de mayo de 2021).

⁹³⁴ Señala además la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2022). “Derecho de supresión (“al olvido”): buscadores de internet”. Disponible en: [https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=el%20derecho%20de%20supresi%C3%B3n%20\('pertinencia%20previstos%20en%20la%20normativa](https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=el%20derecho%20de%20supresi%C3%B3n%20('pertinencia%20previstos%20en%20la%20normativa) (fecha de consulta: 1 de junio de 2022), que, el derecho de supresión (“derecho al olvido”) hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. Véase: derecho de supresión (“al olvido”): buscadores de internet.

⁹³⁵ También aparece en los considerandos 64 y 65 del RGPD.

bajo las cuales aplica⁹³⁶. En este contexto, una persona puede solicitar el derecho de supresión cuando:

- i. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- ii. El interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico;
- iii. El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento;
- iv. Los datos personales hayan sido tratados ilícitamente;
- v. Los datos personales deban suprimirse para el cumplimiento de una obligación legal;
- vi. Que los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8 del RGPD.

Además, el artículo en mención, impone la obligación al responsable del tratamiento de que cuando los datos personales se hayan hechos públicos en un entorno en línea, no solo tiene el deber de borrar los datos, sino también de "adoptar medidas razonables, incluidas las de carácter técnico, para informar a los responsables del tratamiento de los datos personales de que el interesado ha solicitado la supresión por parte de dichos responsables de cualquier enlace a esos datos personales, o de cualquier copia o réplica de los mismos"⁹³⁷. Es decir, el responsable debe tomar medidas razonables, teniendo en cuenta la tecnología disponible y el coste de su aplicación, para

⁹³⁶ STJUE, Sala 2ª, de 13 de mayo de 2014, Asunto: C-131/12, Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, EU:C:2014:317. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12> (fecha de consulta: 5 de junio de 2022).

⁹³⁷ PAGALLO, U., BASSI, E., CREPALDI, M., & DURANTE, M. (2018). "Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure", *JURIX*, p. 86. Disponible en: <https://ebooks.iospress.nl/volumearticle/50837> (fecha de consulta: 20 de mayo de 2022).

informar a otros responsables que procesen datos personales de la solicitud del interesado, para suprimir enlaces y copias o réplicas de esos datos.

No obstante, el derecho al olvido no es absoluto y solo se aplica en determinadas circunstancias específicas, lo que significa, que está condicionado, de manera que, habrá que llevar a cabo “una ponderación de intereses o derechos en conflicto”⁹³⁸, de modo que habrá que examinar cada caso por caso. El responsable del tratamiento es quien asume el riesgo de evaluación del caso, así como la carga de la prueba de la existencia de la excepción⁹³⁹. El RGPD establece 5 causas de exclusión de este derecho:

- i. El derecho a la libertad de expresión e información;
- ii. Para el cumplimiento de una obligación legal o para el cumplimiento una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
- iii. Por razones de interés público en el ámbito de la salud pública;
- iv. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, y
- v. Para la formulación, el ejercicio o la defensa de reclamaciones.

1.2 ¿Qué significa supresión?

El RGPD no define qué significa supresión⁹⁴⁰, por lo que no hay certeza jurídica acerca del alcance de este concepto. Se desconoce qué acciones son suficientes para dar cumplimiento a este derecho. Dependiendo de la interpretación que se le dé, ya sea amplia

⁹³⁸ ALVARES- CARO, M. (2016). “El derecho a la supresión o al olvido”, *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, (Dir. PIÑAR-MAÑAS, J.), Ed.: Reus, p. 250.

⁹³⁹ VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general ...*, Op. Cit., p. 161.

⁹⁴⁰ GIESSEN, D. (2019). *Blockchain and the GDPR's right to erasure*, Bachelor's thesis. Disponible en: <https://essay.utwente.nl/78738/> (fecha de consulta: 20 de junio de 2022). NEUBURGER, J. (2018). “Blockchain, Personal Data and the GDPR Right to be Forgotten”. Disponible en: <https://perma.cc/2XNH-T2GA> (fecha de consulta: 1 de abril de 2022). EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FÓRUM. (2018). *Blockchain An...*, Op. Cit., p. 5. JONGERIUS, S. (2019). “GDPR’s Right to be Forgotten in Blockchain: it’s not black and White”. Disponible en: <https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/> (fecha de consulta: 2 de junio de 2022).

o estricta, la tecnología Blockchain puede entrar o no en conflicto con dicha norma. Es un término que necesita claridad porque como señala el Estudio encargado por el Parlamento Europeo⁹⁴¹, es difícil evaluar si la supresión de datos personales en Blockchain es posible, sin que exista una orientación sobre cómo debe interpretarse. El diccionario de la Real academia de la Lengua Española define derecho al olvido o derecho de supresión como “derecho a eliminar, ocultar y cancelar aquellas informaciones o hechos pasados de la vida de las personas”⁹⁴², lo que sugiere la eliminación de los datos, por lo que, como señala una lectura literal y estricta supone la destrucción completa de los datos⁹⁴³, que en una cadena de bloques pública se realiza mediante una bifurcación dura, que conlleva a:

- i. Una deconstrucción hacia atrás de Blockchain hasta el registro en cuestión.
- ii. Una reconstrucción de la cadena de bloques desde el punto de los datos borrados hacia adelante”⁹⁴⁴.

Para lograr este quiebre se requiere de la cooperación de al menos más de la mitad de los nodos. Sin embargo, aunque se pudiese lograr este consenso y bifurcar para eliminar los datos, estos, aunque en la nueva cadena de bloques ya no existirían, si continuarían estando en la antigua, por lo que dicha información jamás dejaría de existir.

Desde el punto de vista práctico, bifurcar Blockchain no solo es prohibitivamente costoso, sino que parece casi inviable⁹⁴⁵, pero en una cadena de bloques pública, es como señala MEYER, un “evento sísmico y extremadamente raro”⁹⁴⁶, como lo fue en su

⁹⁴¹ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, Op. Cit., p. 75.

⁹⁴² “Derecho al olvido o derecho de supresión” (Sin fecha). Disponible en: <https://dpej.rae.es/lema/derecho-al-olvido-o-derecho-de-supresi%C3%B3n#:~:text=1.,2> (fecha de consulta: 2 de junio de 2022).

⁹⁴³ NEUBURGER, J. (2018). “Blockchain, Personal ...”, cit.

⁹⁴⁴ SHAH, P., FORESTER, D., BERBERICH, M., RASPÉ, C., & MUELLER, H. (2019). “Blockchain technology: Data privacy issues and potential mitigation strategies”. *Practical Law*, p. 6. Disponible en: https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (fecha de consulta: 26 de mayo de 2022).

⁹⁴⁵ BERBERICH, M., & STEINER, M. (2016). “Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers”, *European Data Protection Law Review*, Vol. 2, no. 3, pp. 422-426. Disponible en: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=71&id=&page=> (fecha de consulta: 6 de mayo de 2022).

⁹⁴⁶ MEYER, D. (2018). “Blockchain technology is on a collision course with EU privacy law”, *The Privacy Advisor*. Disponible en: <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/> (fecha de consulta: 15 de abril de 2022).

momento el incidente del DAO. Entonces, tenemos que, en un modelo de Blockchain público existente como Ethereum o bitcoin, es técnicamente casi imposible suprimir los datos almacenados, lo que se traduce en que el derecho al olvido no pueda observarse, por lo menos no de forma directa. Pero no solo eso, sino que también va en contravía de todo lo que representa esta tecnología⁹⁴⁷, a saber, la inmutabilidad.

No obstante, una interpretación más flexible, más allá del borrado material de los datos, puede que permita la aplicación del derecho de supresión en algunos modelos de Blockchain. Aunque es necesario advertir que, dicha tecnología también tendrá que flexibilizar su arquitectura técnica. Por ejemplo, en una interpretación más amplia de este derecho, como en Google España, el TJUE reconoció que la eliminación de los enlaces de los resultados de búsqueda era suficiente para aplicar el derecho al olvido, aunque la solicitud inicial del demandante había sido de eliminar el dato personal del archivo en línea donde se publicó originalmente. Pero como advierte en la doctrina LI, “Este precedente puede indicar que el RGPD exige a los responsables del tratamiento que asuman la responsabilidad del borrado y que esta puede ser otra alternativa para conseguir el “derecho al olvido” cuando exista un obstáculo técnico para aplicarlo directamente”⁹⁴⁸. Es decir, que podría traducirse en que, de acuerdo a lo establecido en el artículo 17.2⁹⁴⁹ puede que el RGPD prescinda de la eliminación material de los datos debido a la imposibilidad técnica de la cadena de bloques para ejecutarlo⁹⁵⁰.

En esta misma línea, algunas autoridades de protección de datos como la francesa y la española han interpretado de forma más matizada la aplicación de este derecho. El CNIL francés advierte que, si bien es técnicamente imposible acceder a la solicitud de supresión realizada por un interesado cuando los datos están registrados en una cadena

⁹⁴⁷ “GDPR Vs. Blockchain – Technology Against The Law”. Disponible en: <https://www.eurolatamlex.com/publications/news/42-gdpr-vs-blockchain-technology-against-the-law.html> (fecha de consulta: 10 de mayo de 2022).

⁹⁴⁸ LI, Z. (2021). “Standardisation of Blockchain...”, *cit.*, p. 10, véase también: EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 75.

⁹⁴⁹ Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

⁹⁵⁰ Véase CASABURO, D. (2022). “Distributed Ledger Technologies and GDPR’s right to be forgotten: Can they get along?”. Disponible en: <https://www.law.kuleuven.be/citip/blog/distributed-ledger-technologies-and-gdprs-right-to-be-forgotten/> (fecha de consulta: 5 de mayo de 2022).

de bloques, reconoce que algunos medios técnicos como el cifrado junto con la destrucción de claves pueden acercarse a un efectivo ejercicio del derecho de supresión para el interesado⁹⁵¹. Por su parte, la Agencia Española de Protección de Datos, en una publicación de información sobre el derecho al olvido, señala que derecho de supresión hace referencia “a impedir la difusión de información personal a través de internet, que incluye el derecho a limitar la difusión universal”⁹⁵². Asimismo, en las directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD, El Comité Europeo de Protección de Datos (CEPD)⁹⁵³, aclara que las solicitudes de supresión de datos personales de los motores de búsqueda no dan lugar a que se supriman completamente los datos y advierte que incluso, los datos personales no se suprimen del sitio web original ni del índice ni de la memoria caché del proveedor de motores de búsqueda, aunque aclara que esto no es absoluto. Si bien estas últimas explicaciones abordan la aplicación del derecho de supresión en relación con los motores de búsqueda, por analogía, estas interpretaciones podrían sugerir que el ejercicio de este derecho no se trata de la eliminación material de los datos, sino de obstaculizar o imposibilitar su divulgación.

No obstante, la cuestión sigue un debate controvertido y no hay seguridad. A falta de una directriz concreta con relación al derecho al olvido en Blockchain por parte del CEPD. Es necesario que, tal y como acertadamente exhorta el Panel para el Futuro de la Ciencia y la Tecnología del Parlamento Europeo, se emita una guía jurídica sobre este tema. Nosotros creemos que el acto de obstaculizar o imposibilitar el acceso de los datos personales debiera considerarse como supresión de datos, pues una interpretación estricta del RGPD no solo supone un problema para Blockchain, sino para otras tecnologías, debido a la dificultad de garantizar que el dato personal pueda ser completamente destruido o eliminado, ya que esto difícilmente puede garantizarse a nivel técnico.

⁹⁵¹ CNIL. (2018). *Solutions for...*, *Op. Cit.*, pp. 8-9.

⁹⁵² AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2022). “Derecho de...”, *cit.*

⁹⁵³ COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2020). “Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD (1.ª parte) Versión 2.0 Adoptadas el 7 de julio de 2020”. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbsearchengines_afterpublicconsultation_es.pdf (fecha de consulta: 6 de junio de 2022).

1.3 Soluciones técnicas

Suprimir datos en una Blockchain pública sin comprometer características técnicas fundamentales que subyacen dicha tecnología, es casi imposible⁹⁵⁴. Para los puristas y partidarios de las criptomonedas, la inmutabilidad y la arquitectura distribuida constituyen una de las propiedades más deseadas⁹⁵⁵, pues en ellas se basa la confianza “sin confianza”. En efecto, el registro inmutable, transparente y distribuido de los datos, facilita el almacenamiento de información de forma segura, auditable y creíble⁹⁵⁶. En virtud de estas propiedades, teóricamente en las cadenas de bloques públicas, el derecho al olvido no puede ejercerse, primero porque no hay un responsable del tratamiento, destinatario de la solicitud de olvido por parte del interesado, y segundo porque una bifurcación no solo requiere de la cooperación de más de la mitad de los miembros de la red, sino porque demanda de recursos técnicos costosos. Es inviable concebir reescribiendo bitcoin o Ethereum cada vez que un usuario haga una solicitud de olvido.

No obstante, la industria y la academia han propuesto el diseño de soluciones técnicas en las cuales se flexibilizan las propiedades clave de dicha tecnología. Por supuesto, aquí hay de nuevo lugar para ciertas preocupaciones y constituye un tema objeto de debate. En primer lugar, la capacidad de cumplimiento del RGPD por parte de estas soluciones y, por otra parte, la relajación de las características claves de las cadenas de bloques, aunque tecnológicamente sea posible.

A continuación, abordaremos las principales propuestas que han surgido, para ello, es importante recordar la distinción de los datos almacenados en Blockchain, los datos transaccionales y las claves públicas.

⁹⁵⁴ TATAR, U., GOKCE, Y., & NUSSBAUM, B. (2020). “Law versus technology: Blockchain, GDPR, and tough tradeoffs”, *Computer Law & Security Review*, Vol. 38. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0267364920300595> (fecha de consulta: 23 de mayo de 2022).

⁹⁵⁵ COMPERT, C., LUINETTI, M., & PORTIER, B. (2018). “Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance”, *IBM Security White Paper*. p. 3. Disponible en: <https://iapp.org/resources/article/blockchain-and-gdpr/> (fecha de consulta: 16 de mayo de 2022).

⁹⁵⁶ POLITOU, E., ALEPIS, E., VIRVOU, M., PATSAKIS, C. (2022). “Privacy in Blockchain”, *Privacy and Data Protection Challenges in the Distributed Era. Learning and Analytics in Intelligent Systems*, (Drs. POLITOU, E., ALEPIS, E., VIRVOU, M., PATSAKIS, C.), Ed.: Springer, Cham, p. 135. Disponible en: https://doi.org/10.1007/978-3-030-85443-0_7 (fecha de consulta: 26 de mayo de 2022).

1.3.1 Almacenar información de identificación personal fuera de Blockchain

Una de las técnicas que se ha propuesto es guardar los datos de carácter personal fuera de la cadena de bloques⁹⁵⁷, almacenando en esta un *hash* que se vincula a una base de datos externa que contiene la información completa⁹⁵⁸. Por ejemplo, una Blockchain que incluye datos personales como, nombre, identificación e información de salud de un determinado grupo de personas, en lugar de almacenar esta información en la cadena, se opta por guardar un *hash* generado a partir de los datos que contiene, de tal manera, que lo que se visualiza en el bloque será una secuencia de caracteres alfanuméricos. De forma similar, la CNIL⁹⁵⁹ recomienda nunca guardar directamente datos personales dentro de Blockchain y considera que la información no cifrada debe registrarse como un esquema de compromiso.

Cuando el interesado solicita ejercer su derecho de supresión frente al encargado del tratamiento, los datos se eliminan de la base de datos, con lo cual se estaría dando cumplimiento al artículo 17 del RGPD. Esto hace que el *hash* en la cadena de bloques sea inútil para fines de identificación⁹⁶⁰.

Sin embargo, esta solución no está exenta de críticas, ya que introduce los mismos problemas de las bases de datos tradicionales, la no resistencia a la manipulación⁹⁶¹, la

⁹⁵⁷ READ, I. I., & PEHLIVAN, C. N. (2020). "Blockchain and Data Protection: A Compatible Couple?", *Global Privacy Law Review*, Vol. 1. No. 1, p. 47 Disponible en: https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/1.1/GPLR2020005_05 (fecha de consulta: 8 de junio de 2022). GOLDEN DATA LAW (2019) "Blockchain: Challenges and solutions for compliance with the GDPR" Disponible en: <https://medium.com/golden-data/blockchain-challenges-and-solutions-for-compliance-with-the-gdpr-c354987f8fae> (fecha de consulta: 3 de abril de 2022).

⁹⁵⁸ PAGALLO, U., BASSI, E., CREPALDI, M., & DURANTE, M. (2018). "Chronicle ...", *cit.*, p. 86. Véase también IBÁÑEZ, L. D., O'HARA, K., & SIMPERL, E. (2018) "On blockchains and the general data protection regulation", *EU Blockchain Forum and Observatory*, p. 8. Disponible en: https://eprints.soton.ac.uk/422879/1/BLOCKchains_GDPR_4.pdf (fecha de consulta: 2 de diciembre de 2021).

⁹⁵⁹ DAOUI, S., FLEINERT-JENSEN, T., & LEMPERIERE, M. (2019). "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions", *Stanford Journal of Blockchain Law & Policy*, vol 2. Disponible en: <https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france/release/1> (fecha de consulta: 2 de mayo de 2022). MARTIN-BARITEAU, F. (2018). "Blockchain and the European union general data protection regulation: The CNIL's perspective", *Blockchain Working Paper Series*, 1, p. 10. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275783 (fecha de consulta: 2 de mayo de 2022).

⁹⁶⁰ MIRCHANDANI, A. (2019). "The GDPR-blockchain paradox: exempting permissioned Blockchains from the GDPR", *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 29, No. 4, p.1229. Disponible en: <https://ir.lawnet.fordham.edu/iplj/vol29/iss4/5/> (fecha de consulta: 2. De mayo de 2022).

⁹⁶¹ EBERHARDT, J., TAI, S. (2017). "On or Off the Blockchain? Insights on Off-Chaining Computation and Data" *European Conference on Service-Oriented and Cloud Computing*, (Drs. DE PAOLI, F., SCHULTE, S., BROCH JOHNSON, E.), Ed.: Springer, Cham. Disponible en: https://doi.org/10.1007/978-3-319-67262-5_1 (fecha de consulta: 9 de junio de 2022).

vulnerabilidad a los ataques⁹⁶² y la centralización; además, para operar necesita de la presencia de un tercero intermediario. Algunos autores⁹⁶³ han considerado que es una traición a la descentralización de las cadenas de bloques, por el hecho de que parte del control de la información se encuentre centralizada o, incluso, algunos⁹⁶⁴ han cuestionado la necesidad de emplear la tecnología Blockchain, ya que hace al sistema más complejo e ineficiente.

Almacenar o no datos en Blockchain continúa siendo un tema controvertido, pues contrario a lo que se piensa, no es tarea fácil. De hecho, almacenar la referencia *hash* de los datos en lugar de los datos en sí, parece ser la solución más sensata, aunque evidentemente las claves públicas que, pueden calificar como datos personales, no se pueden almacenar externamente⁹⁶⁵, lo que representa un obstáculo para su aplicación. Así como el hecho de que los *hashes* sean considerados en algunas ocasiones como datos seudónimos, aunque como hemos mencionado, haya que analizar cada caso por individual para determinarlo.

Sin embargo, almacenar datos directamente en una cadena de bloques es costoso y está limitado por el protocolo (la mayoría permite almacenar en el rango de *kilobytes* o menos), debido a que, cada dato que se almacena tiene que ser guardado por cada nodo que la descarga (cada participante tiene una copia local), razón por la cual, guardar un kilobyte puede llegar a ser costoso⁹⁶⁶. Es más, una Blockchain, en lugar de parecerse más a una base de datos, es más bien como un archivo de registro. Prueba de ello, son los famosos NFTs, ya que en la red Ethereum no se guarda la imagen u obra artística como tal, sino un enlace del contenido que representan⁹⁶⁷. Así que, aunque haya preocupaciones

⁹⁶² Véase STEINBECK, D. (2028). “How New EU Privacy Laws Will Impact Blockchain: Expert Take”. Disponible en: <https://cointelegraph.com/news/how-new-eu-privacy-laws-will-impact-blockchain-expert-take> (fecha de consulta: 9 de junio de 2022). HUMBEECK, A. V. (2019). The blockchain-GDPR paradox. Disponible en: <https://blog.codemine.be/posts/20171121-blockchain-gdpr-paradox/> (fecha de consulta: 5 de junio de 2022).

⁹⁶³ O'HARA, K., & SIMPERL, E. (2018) “On blockchains ...”, *cit.*, p. 8.

⁹⁶⁴ MIRCHANDANI, A. (2019). “The GDPR...”, *cit.*, p. 1230.

⁹⁶⁵ Véase MATSSON, D. (2022). *GDPR, Blockchain & Personal data-The rights of the individual v. the integrity of Blockchain*. P. 47. Disponible en: https://gupea.ub.gu.se/bitstream/handle/2077/70713/gupea_2077_70713_1.pdf;jsessionid=71E241E80D447BE6170AFAAF6CD2E8C7?sequence=1 (fecha de consulta: 9 de junio de 2022).

⁹⁶⁶ MARX, L. (2018). “Storing Data on the Blockchain: The Developers Guide”. Disponible en: <https://malcoded.com/posts/storing-data-blockchain/> (fecha de consulta: 5 de junio de 2022).

⁹⁶⁷ ROSENTHAL, D. (2021). “NFTs and Web Archiving”. Disponible en: <https://blog.dshr.org/2021/04/nfts-and-web-archiving.html> (fecha de consulta: 7 de junio de 2022).

con respecto a los principios filosóficos de dicha tecnología, esta es la única manera eficiente y económica de gestionar información en Blockchain.

1.3.2 Destrucción de claves de cifrado

Otra solución que se ha planteado es emplear un esquema de cifrado con clave⁹⁶⁸ para los datos, ya sea que estos estén almacenados dentro o fuera de Blockchain⁹⁶⁹. Para dar cumplimiento al derecho de supresión, la clave secreta se destruye, pues al hacerlo es extremadamente difícil descifrar el texto cifrado⁹⁷⁰. Esta técnica fue propuesta por la Autoridad francesa de protección de datos⁹⁷¹, al sugerir en su informe que, la supresión podría obtenerse cuando se elimina la clave secreta de la función *hash* codificada. Si bien aclara que, aunque estrictamente hablando, no es supresión, en la medida que los datos continúan existiendo en la cadena, el estudio advierte que, esto permite acercarse a un ejercicio efectivo del derecho de supresión para el interesado. De tal forma que, la efectividad de esta técnica depende del tipo de interpretación que se le dé al artículo 17, esto es, si los datos inaccesibles constituyen supresión.

Esta propuesta también presenta problemas de seguridad, ya que con un método de prueba y error se puede encontrar la clave secreta⁹⁷² (ataques de fuerza bruta) y adicionalmente, hay que tener en cuenta el desarrollo tecnológico⁹⁷³, pues los sistemas de cifrado actuales no son tan seguros de cara a los avances de la computación cuántica. Según el dictamen sobre técnicas de anonimización, el Grupo de Trabajo del artículo 29 señala que, la destrucción de claves no elimina la posibilidad de reidentificar al interesado y advierte que, “la mera implementación de una traducción semántica de datos personales (el caso de la codificación con clave) no descarta la posibilidad de revertir los datos a su estructura original, ya sea aplicando el algoritmo en sentido inverso o mediante ataques de fuerza bruta, según la naturaleza de los sistemas, o como resultado de la violación de

⁹⁶⁸ Véase DE MEIJER, C. (2018). “Blockchain versus GDPR and who should adjust most”. Disponible en: <https://www.finextra.com/blogposting/16102/blockchain-> (fecha de consulta: 12 de junio de 2022). O’HARA, K., & SIMPERL, E. (2018) “On blockchains ...”, *cit.*, p. 8. EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. (2018). *Blockchain An...*, *Op. Cit.*, p. 25.

⁹⁶⁹ BACON, J., MICHELS, J. D., MILLARD, C., & SINGH, J. (2018). “Blockchain demystified ...”, *cit.*, p. 76.

⁹⁷⁰ BAYLE, A., KOSCINA, M., MANSET, D., & PEREZ-KEMPNER, O. (2018). “When blockchain ...”, *cit.*, p. 3.

⁹⁷¹ MARTIN-BARITEAU, F. (2018). “Blockchain and...”, *cit.*, p. 10.

⁹⁷² BAYLE, A., KOSCINA, M., MANSET, D., & PEREZ-KEMPNER, O. (2018). “When blockchain ...”, *cit.*, p. 3.

⁹⁷³ PAGALLO, U., BASSI, E., CREPALDI, M., & DURANTE, M. (2018). “Chronicle ...”, *cit.*, p. 92.

los datos. Los sistemas de cifrado más avanzados garantizan que los datos reciben la máxima protección.”⁹⁷⁴. Como acertadamente señalan PAGALLO y otros, aquí la confrontación se da no por una cuestión de principios, sino por seguridad⁹⁷⁵, dado que en un futuro pueden estar en riesgo.

1.3.3 Hash camaleónico- mutabilidad

Otra solución que se ha planteado para cumplir con los requisitos del artículo 17 del Reglamento General de Protección de Datos⁹⁷⁶, es la mutabilidad de la cadena de bloques, que permite que los datos se puedan modificar o eliminar. Para ello se utiliza una función *hash* camaleón, que consiste en una función *hash* que implica una puerta trampa (o clave secreta), cuyo conocimiento permite encontrar colisiones arbitrarias en el dominio de la función. Sin embargo, las funciones *hash* camaleón son resistentes a las colisiones (no es posible producir el mismo *hash* a partir de entradas diferentes) siempre que no se conozca la correspondiente puerta trampa. Más concretamente, una parte que conozca la trampilla es capaz de encontrar colisiones arbitrarias en el dominio de la función⁹⁷⁷, lo que supone que se pueda reescribir el contenido del bloque. En otras palabras, una función *hash* camaleón implica agregar un candado a cada eslabón de la cadena, si no se tiene la llave que la desbloquea, es difícil encontrar colisiones, por lo que, si esta se pierde o se destruye, la Blockchain vuelve a ser inmutable⁹⁷⁸. Es decir, con el conocimiento de la clave secreta, es posible modificar, insertar o eliminar cualquier bloque⁹⁷⁹, sin cambiar el resultado de la función *hash*⁹⁸⁰, por lo que se pueden borrar datos

⁹⁷⁴ UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014 sobre técnicas de anonimización*, p. 33. Disponible en <https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf> (fecha de consulta: 17 de junio de 2021).

⁹⁷⁵ PAGALLO, U., BASSI, E., CREPALDI, M., & DURANTE, M. (2018). “Chronicle ...”, *cit.*, p. 92.

⁹⁷⁶ VALPĪTERE, M. (2020). “Right to erasure” and private blockchain in the European Union: legal requirements and technical possibilities, Bachelor thesis, p. 35. Disponible en: https://dspace.lu.lv/dspace/bitstream/handle/7/52535/Valpitere_Marina.pdf?sequence=1 (fecha de consulta: 10 de mayo de 2022). GIESSEN, D. (2019). *Blockchain ...*, *Op. Cit.*, p. 5.

⁹⁷⁷ CAMENISCH, J., DERLER, D., KRENN, S., PÖHLS, H.C., SAMELIN, K., SLAMANIG, D. (2017). “Chameleon-Hashes with Ephemeral Trapdoors” *ACR International Workshop on Public Key Cryptography*, (Dirs. FEHR, S.), Ed.: Springer, Berlin, Heidelberg. Disponible en: https://doi.org/10.1007/978-3-662-54388-7_6 (fecha de consulta: 20 de junio de 2022).

⁹⁷⁸ ATENIESE, G., MAGRI, B., VENTURI, D., & ANDRADE, E. (2017) “Redactable blockchain—or—rewriting history in bitcoin and friends”, *2017 IEEE European symposium on security and privacy*, p. 112. Disponible en: <https://ieeexplore.ieee.org/document/7961975> (fecha de consulta: 21 de junio de 2022).

⁹⁷⁹ GRICENKO, T. (2020). *Blockchain technology: edit or not?* MSc Research Project, p. 8. Disponible en: <https://norma.ncirl.ie/4562/1/tatyanagricenko.pdf> (fecha de consulta: 21 de junio de 2022).

⁹⁸⁰ MOEREL, L. (2019). “Blockchain and...”, *cit.*, p. 230.

personales de la red. No obstante, cuando se produce la modificación queda una “cicatriz” que indica que se ha alterado el bloque, lo que significa que la cadena de bloques se mantiene transparente y verificable⁹⁸¹.

El *hash* camaleón debe ser empleado por quienes conozcan la clave secreta. Se ha sugerido que dicho conocimiento puede estar en cabeza de mineros, jueces, árbitros o un auditor centralizado⁹⁸², pero no se ha llegado aún consenso sobre quien debe poseer dicha clave, esto continúa siendo un debate abierto. No obstante, estas ideas entran en conflicto con los principios de la tecnología, pues una Blockchain que no sea inmutable y que reintroduzca terceros de confianza al sistema hace que se reconsidere cuál podría ser el objetivo emplear una cadena de bloques si se abandonan sus características principales⁹⁸³.

1.4 Consideraciones

Además de las soluciones técnicas antes mencionadas, se han sugerido otros remedios como la anonimización de los datos o la poda, que permite la verificación de un nuevo bloque sin procesar todo el historial de transacciones⁹⁸⁴, lo que permite eliminar transacciones obsoletas⁹⁸⁵, sin embargo, también han sido objeto de críticas, ya que su aplicabilidad no es estable, pues esto depende de la voluntad de los nodos⁹⁸⁶.

Tras el estudio que hemos realizado, podemos concluir que todas las soluciones presentan inconvenientes, ya sea por razones jurídicas como, por ejemplo, que no haya claridad acerca de lo que se entiende por supresión, o porque se renuncia a los principios filosóficos de la tecnología Blockchain, como es tener que hacer modificaciones en la cadena o la introducción de un tercero de confianza. No obstante, no se puede decir de

⁹⁸¹ POLITOU, E., ALEPIS, E., VIRVOU, M., PATSAKIS, C. (2022). “Privacy in...”, *cit.*, p. 140, véase Tambien GRICENKO, T. (2020). *Blockchain technology...*, *Op. Cit.*, p. 8.

⁹⁸² ATENIESE, G., MAGRI, B., VENTURI, D., & ANDRADE, E. (2017). “Redactable blockchain...”, *cit.*, p. 113.

⁹⁸³ Véase: GREENSPAN, G (2017). “The blockchain immutability myth”. Disponible en: <https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/> (fecha de consulta: 21 de junio de 2022). LI, Z. (2021), “Standardisation of Blockchain...”, *cit.*, p. 10. EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 33, VALPÍTERE, M. (2020). “*Right to erasure*” and private, *Op. Cit.*, p. 35.

⁹⁸⁴ MOEREL, L. (2019). “Blockchain and...”, *cit.*, p. 229, EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 35.

⁹⁸⁵ MANTEGHI, M. (2021). “Blockchain and...”, *cit.*, p. 16.

⁹⁸⁶ GRICENKO, T. (2020). *Blockchain technology...*, *Op. Cit.*, p. 8.

plano que el derecho al olvido es en sí mismo incompatible con la cadena de bloques, pues existe una variedad de diseños de las misma, con lo cual dependerá de la arquitectura de cada una, lo que permitirá establecer si se puede aplicar o no el derecho al olvido, es por eso que se tiene que analizar cada caso concreto. No obstante, las técnicas propuestas tienen cabida en Blockchains privadas con permiso, por lo que, a día de hoy, no es posible aplicar el derecho al olvido a redes públicas y sin permiso como lo puede ser Ethereum o Bitcoin, es más ni siquiera hay claridad ante quien se puede ejercer este derecho.

2. Derecho de rectificación

Establece el artículo 16 del RGPD que el “el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional”. Este derecho tiene por objetivo corregir o evitar los efectos negativos⁹⁸⁷ de los datos inexactos que atañen a los interesados. El RGPD no define qué significa datos inexactos, sin embargo, podría decirse que son datos que son incorrectos, engañosos o que no son ciertos ⁹⁸⁸, es decir, que no reflejan la realidad. En cuanto a los datos incompletos, señala el Reglamento que, teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen, por lo que solo deben completarse cuando se necesite alcanzar los fines del tratamiento⁹⁸⁹.

Como podemos observar, este derecho implica la alteración de los datos, ya sea para rectificarlos o para completarlos, por lo que nuevamente la inmutabilidad de la tecnología Blockchain hace que sea problemática su aplicación. Recordemos, que el diseño de una cadena de bloques tiene como propósito hacer que los datos almacenados sean inalterables y no se puedan modificar. Al igual que con el derecho al olvido, no hay claridad ante quién debe acudir el interesado para el ejercicio de su derecho, ya que los nodos no tienen capacidad de cambiar los datos almacenados en un bloque⁹⁹⁰ (caso

⁹⁸⁷ VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general ...*, Op. Cit., p. 154.

⁹⁸⁸ GOLDEN DATA LAW. (2019). “Right to rectification under EU data protection law”. Disponible en: <https://medium.com/golden-data/right-to-rectification-35ec099df2fc> (fecha de consulta: 20 de junio de 2022).

⁹⁸⁹ VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general ...*, Op. Cit., p. 155.

⁹⁹⁰ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, Op. Cit., p. 21.

contrario ocurría en una red privada y con permiso). Aunque en teoría la mitad más uno de los nodos puede alterar el historial de transacciones, tal y como mencionamos en la sección sobre el derecho de supresión, esto supone una bifurcación dura, lo cual es un evento excepcional y, aun así, aunque se bifurque, los datos seguirían existiendo.

La autoridad francesa de protección de datos⁹⁹¹, señala de plano que es técnicamente e imposible conceder la solicitud de rectificación porque, incluso si se ingresa un nuevo bloque en la cadena con la información correcta, el bloque anterior, el cual contiene los datos inexactos, aún seguirá apareciendo en la Blockchain⁹⁹². Sin embargo, el reglamento permite que los datos incompletos se completen mediante una declaración adicional, por lo que, es posible que esta opción sea viable en una cadena de bloques, pues un tercero podría agregar información que complete los datos. Si esa solución cumple o no con el artículo 16, continúa en discusión⁹⁹³. Es importante destacar que esta solución no aplica a la modificación de los datos inexactos, por lo que se ha sugerido que los datos se almacenen por fuera de la cadena o el empleo de *hashes* camaleónicos, sin embargo, al igual que sucede con el derecho al olvido estas soluciones presentan problemas de seguridad e ideológicos (introducción de terceros y mutabilidad).

Creemos que el derecho de rectificación no es incompatible con Blockchain, sino que algunos diseños de cadenas de bloques públicas hacen que no se pueda cumplir, pues la inmutabilidad en estas arquitecturas suele ser un punto inflexible e innegociable. En cambio, en las privadas puede ser más factible cumplir con este derecho, ya que sus desarrolladores pueden incluir herramientas técnicas y mecanismos de gobernanza que así lo permitan.

⁹⁹¹LI, Z. (2021). “Standardisation of Blockchain...”, *cit.*, p. 11.

⁹⁹² “Blockchain and GDPR: beyond the right to be forgotten”. (2018). Disponible en: <https://www.osborneclarke.com/insights/blockchain-gdpr-beyond-right-forgotten> (fecha de consulta: 21 de junio de 2022).

⁹⁹³MANTEGHI, M. (2021). “Blockchain and...”, *cit.*, p. 15.

IV.TENSIÓN Y PRINCIPIOS MINIMIZACIÓN DE DATOS Y LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

El RGPD establece 7 principios relativos al tratamiento de los datos, que determinan, como razonablemente señala MONTERO⁹⁹⁴, cómo se debe recoger, tratar y ceder los datos personales, con el objetivo de garantizar la privacidad de los interesados. De estos principios, dos parecen ser que entran en conflicto con la inmutabilidad de la tecnología Blockchain: la minimización de datos y la limitación del plazo de conservación. En cuanto al primero, se trata de que los datos personales deben ser “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”⁹⁹⁵. Esto es, no se trata de minimizar el tratamiento al mínimo absoluto, sino más bien de minimizar la recogida en relación con los fines del tratamiento⁹⁹⁶.

En cuanto al principio de limitación del plazo de conservación⁹⁹⁷, se basa en la premisa que los datos personales no pueden almacenarse por períodos ilimitados⁹⁹⁸. Es decir, que los datos deben conservarse durante un tiempo que no sea superior al necesario para los fines del tratamiento, por lo que los datos no se pueden almacenar de forma indefinida. Esta disposición se reafirma con la obligación que tiene el responsable del tratamiento de supresión estipulado en el artículo 17⁹⁹⁹.

El principio de minimización de datos desafía la naturaleza acumulativa y replicada de Blockchain, pues cada nodo guarda una copia de la base de datos¹⁰⁰⁰. Y cada bloque contiene el historial de todas las transacciones, por lo que la cantidad de datos almacenados es exagerada, sin embargo, ello garantiza la integridad y la

⁹⁹⁴ MONTERO-PUYOL, F. (2016). “Los principios del derecho a la protección de datos”, *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, (Dirs. PIÑAR-MAÑAS, J.), Ed.: Reus, p. 135.

⁹⁹⁵ Artículo 5 c RGPD.

⁹⁹⁶ P VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general ...*, Op. Cit., p. 90.

⁹⁹⁷ Artículo 5E. e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se trate exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»).

⁹⁹⁸ <https://medium.com/golden-data/blockchain-challenges-and-solutions-for-compliance-with-the-gdpr-c354987f8fae>

⁹⁹⁹ P VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general ...*, Op. Cit., p.92.

¹⁰⁰⁰ MANTEGHI, M. (2021). “Blockchain and...”, *Cit.*, p. 13, EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, Op. Cit., p. 80.

descentralización. Todo ello almacenado de forma permanente e inmutable, con lo cual no hay lugar a su eliminación o modificación, lo que supone que los datos innecesarios recopilados en exceso no se pueden eliminar¹⁰⁰¹.

En cuanto al principio de limitación del plazo de conservación, choca el hecho de que la arquitectura de las cadenas de bloques esté diseñada para que se pueda verificar la integridad de la información, lo cual implica que cada bloque contiene todas las transacciones que se han hecho en su historia. De tal manera, que los datos siempre se estarán procesando de forma permanente, sin poderse modificar o eliminar. Lo que significa que los mismos no se pueden borrar cuando ya no son necesarios.

Teniendo en cuenta estos desafíos, es necesario cuestionarse si la cadena de bloques es compatible con estos principios. A primera vista pareciese que no, sin embargo, tal y como hemos mencionado, esta respuesta depende de las circunstancias de diseño de cada Blockchain, pues cada desarrollo tiene sus propias particularidades. La respuesta no sería la misma en una cadena de bloques autorizada, donde el administrador podría tener ciertas facultades que le permitirían editar la misma, que, en Ethereum, una plataforma que necesita de un mecanismo de gobernanza que cuente con más de la mitad de sus participantes.

Pero no debemos dejar de lado que el principio de minimización de datos no solo se refiere a la cantidad de datos, sino a la calidad de los mismos¹⁰⁰². Es más, algunos autores señalan que el factor determinante es la calidad, razón por la cual el principio de minimización de datos no es incompatible con la tecnología Blockchain. Como READ Y PEHLIVAN¹⁰⁰³, que sostienen que, si se tiene en cuenta que la distribución de los datos en una cadena es necesaria para su funcionamiento, y que estos se limitan solo a aquellos que son imprescindibles para la finalidad del tratamiento para el que se recoge, este principio no se ve afectado. No obstante, como acertadamente advierte el estudio del Parlamento Europeo¹⁰⁰⁴, esto parece poco probable, pues según el artículo 25 del RGPD,

¹⁰⁰¹ FINCK, M. (2017). "Blockchains and Data...", *cit.*, p. 21.

¹⁰⁰² EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 68.

¹⁰⁰³ READ, I. I., & PEHLIVAN, C. N. (2020). "Blockchain and Data...", *cit.*, p. 46.

¹⁰⁰⁴ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 68.

el responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas para garantizar, por defecto, que solo sean objeto del tratamiento solo los datos que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

También existen soluciones técnicas que matizan y pueden compatibilizar dicha tecnología con el Reglamento, como almacenar los datos por fuera de la cadena, aunque nuevamente surgirían los interrogantes acerca de la necesidad de usar esta tecnología si se van a guardar los datos externamente.

Sin embargo, el mayor desafío sigue siendo conciliar estos principios con las claves públicas¹⁰⁰⁵, pues para el funcionamiento de una cadena de bloques, estas siempre deben estar visibles, por lo que tal y como advierte la CNIL no se pueden minimizar y su período de retención estará en línea con la vida de la cadena de bloques¹⁰⁰⁶.

V.RESPOSABLE DEL TRATAMIENTO

Según el artículo 4. (7) del Reglamento, el responsable del tratamiento (también llamado responsable) es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Es decir, es quien determina el por qué y el cómo de las actividades del tratamiento¹⁰⁰⁷. En este sentido, señala SANTOS que el por qué y el cómo incluyen, “la determinación de qué datos van a ser objeto de tratamiento, las operaciones que van a realizarse con ellos y quiénes tendrán acceso a esos datos”¹⁰⁰⁸, así como aspectos técnicos como el *hardware* o *software* que van a emplearse.

¹⁰⁰⁵ FINCK, M. (2017). “Blockchains and Data...”, *cit.*, p. 21.

¹⁰⁰⁶ JAMBERT, A. (2019). “Blockchain and the GDPR: A data protection authority point of view” *Information Security Theory and Practice 12th IFIP International Conference*, (Dirs. BLAZY, O., & YEUN, C), Ed.: Springer, Cham. Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-20074-9_1 (fecha de consulta: 1 de junio de 2022).

¹⁰⁰⁷ EUROPEAN UNION, ARTICLE 29 DATA PROTECTION WORKING PARTY (2010). Opinion 1/2010 on the concepts of “controller” and “processor”. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (fecha de consulta: 25 de junio de 2022).

¹⁰⁰⁸ SANTOS-MORÓN, M. J. (2020). “Tratamiento de datos...”, *cit.*, p. 37.

El RGPD fue escrito con un control central en mente¹⁰⁰⁹, el encargado del tratamiento, el cual tiene asignada la responsabilidad de la protección de los datos y es ante quien el interesado acude a ejercer sus derechos. Por lo tanto, para dar cumplimiento al Reglamento, el responsable tratamiento debe estar plenamente identificado.

No obstante, Blockchain opera como una red distribuida, resultado de una cooperación entre pares¹⁰¹⁰ (*peer-to-peer*) repartidos alrededor del mundo. Los participantes actúan al mismo tiempo como servidor y como cliente¹⁰¹¹. Es decir, que los usuarios se comunican y colaboran de forma directa y sin necesidad de un punto central, de modo que, distinguir al responsable del interesado, se vuelve problemático, pues existe una línea borrosa que los separa, pues en una cadena de bloques todos actúan y son considerados como iguales¹⁰¹², aunque tengan funciones diferentes en la forma en como apoyan a la red¹⁰¹³.

Como siempre, la respuesta depende del diseño de la cadena de bloques. En redes privadas va a resultar más fácil identificar al responsable del tratamiento, pues el administrador de la misma en principio calificaría como el responsable del tratamiento. Por ejemplo, si una empresa de certificación de documentos digitales emplea la tecnología Blockchain y para llevar a cabo su labor necesita procesar datos, pues esa compañía se considerará como el responsable del tratamiento, por lo que dicha empresa calificaría como la responsable del tratamiento.

En este contexto, el desafío más interesante surge al analizar Blockchain públicas y sin permiso, pues funcionan como una red distribuida y descentralizada conformada por una multiplicidad de actores. No existe un punto central que pueda calificar como el responsable. En principio, todos los nodos podrían ser considerados como responsable

¹⁰⁰⁹ SPREY, J. (2019.) "Blockchain and the controller under the GDPR: finding a necessary balance for BC to become a mainstream infrastructure". Disponible en: <https://www.vwsadvocaten.nl/en/blockchain-and-the-gdpr-data-controllers-and-data-processors/> (fecha de consulta: 24 de junio de 2022).

¹⁰¹⁰ BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). "Bitcoin and the...", *cit.*, p. 192.

¹⁰¹¹ SCHOLLMEIER, R. (2002). "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," *Proceedings First International Conference on Peer-to-Peer Computing*, p. 101. Disponible en: <https://ieeexplore.ieee.org/document/990434> (fecha de consulta: 10 de mayo de 2022).

¹⁰¹² CLIFFORD CHANCE. (2018). *Global intellectual property newsletter Blockchain, AI and other IP topics*, Vol. 3, p. 25. Disponible en: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2018/03/global-intellectual-property-newsletter-17th-issue-blockchain-ai-and-other-ip-topics.pdf> (fecha de consulta: 23 de mayo de 2022).

¹⁰¹³ READ, I. I., & PEHLIVAN, C. N. (2020). "Blockchain and Data...", *cit.*, p. 42.

del tratamiento debido a su acción, y al mismo tiempo pueden ser considerados encargados del tratamiento debido a la copia que guardan de la cadena de bloques¹⁰¹⁴.

Para poder dar respuesta acerca de quién podría calificar como responsable del tratamiento de datos, es necesario analizar las partes involucradas y sus aportes a la red. Habida cuenta que existen múltiples proyectos de Blockchain y que cada caso debe analizarse de forma individual¹⁰¹⁵. En esta sección tomaremos como referencia una cadena de bloques pública que utilice la prueba de trabajo (aplicaría también para la prueba de participación) y donde cualquier persona de forma libre pueda convertirse en nodo, como en el caso de Bitcoin.

1. Desarrolladores

Estos sujetos son los responsables de desarrollar el código con el que opera una cadena de bloques y del diseño de su arquitectura. Por ejemplo, en bitcoin el código original fue escrito por SATOSHI NAKAMOTO y actualmente cualquier persona puede colaborar de forma voluntaria en el desarrollo del *software*, pero solo unos pocos tienen acceso al desarrollo de Core¹⁰¹⁶, (es un *software* de Código abierto responsable del protocolo de bitcoin)¹⁰¹⁷, los llamados desarrolladores principales. No obstante, las decisiones sobre los cambios en el código deben ser aprobados por la mayoría de nodos, quienes deciden si implementan una actualización o no. Como señalan NARAYANAN y otros, “Los desarrolladores principales pueden instar a la comunidad, pero no tienen poder formal para obligar a la gente a seguirles si llevan el sistema en una dirección técnica que no gusta a la comunidad”¹⁰¹⁸. Esto sucede de forma parecida en otros desarrollos Blockchain de criptomonedas.

¹⁰¹⁴ Véase: BAYLE, A., KOSCINA, M., MANSET, D., & PEREZ-KEMPNER, O. (2018). “When blockchain ...”, *cit.*, p. 2.

¹⁰¹⁵ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain....*, *Op. Cit.*, p. 4.

¹⁰¹⁶ NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., & GOLDFEDER, S. (2016). *Bitcoin and....*, *Op.Cit.*, p. 250.

¹⁰¹⁷ “Qué es Bitcoin Core”. (2020). Disponible en: <https://academy.bit2me.com/que-es-bitcoin-core/> (fecha de consulta: 23 de mayo de 2021).

¹⁰¹⁸ NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., & GOLDFEDER, S. (2016). *Bitcoin and....*, *Op.Cit.*, p. 251.

Sin embargo, no están involucrados la actividad diaria de la cadena¹⁰¹⁹ así que su papel es limitado en los medios de procesamiento, pues ellos solo establecen las reglas, y la estructura de gobierno es la que decide utilizarla para sus propios propósitos¹⁰²⁰. Por lo tanto, habida cuenta que no establecen ni el por qué, ni el cómo del tratamiento, no pueden ser responsable del mismo¹⁰²¹.

2. Mineros

Los mineros son un tipo de nodo de vital importancia en este desarrollo tecnológico, pues se encargan agregar nuevos bloques y validar las transacciones de acuerdo a las reglas de la red (por ejemplo, prueba de trabajo o prueba de participación). A cambio de su labor reciben una compensación económica, que en el caso de Blockchain de criptomonedas, generalmente, son monedas recién acuñadas¹⁰²². Es decir, que su labor es técnica y su objetivo es incluir bloques en la cadena y que las copias de esta estén sincronizadas¹⁰²³, pero lo hace ciñéndose a los protocolos establecidos en el código de la Blockchain.

A pesar de que su labor es de gran importancia, los mineros no determinan los fines y medios del tratamiento, pues como señala la CNIL, los mineros solo validan las transacciones enviadas por los participantes y no están involucrados con el objeto de estas transacciones¹⁰²⁴, su papel se limita a procesarlas mecánicamente¹⁰²⁵. Advierte el estudio del Parlamento Europeo que, su función se ha comparado con la de un administrador de

¹⁰¹⁹ SCHELLEKENS, M. (2020). "Conceptualizations of the controller in permissionless blockchains", *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 11. Disponible en: <https://www.jipitec.eu/issues/jipitec-11-2-2020/5099> (fecha de consulta: 1 de julio de 2022).

¹⁰²⁰ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 46.

¹⁰²¹ Estos autores opinan que los desarrolladores no son responsables del tratamiento, véase BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). "Bitcoin and the...", *cit.*, p. 195. BACON, J., MICHEL, S. D., MILLARD, C., & SINGH, J. (2018). "Blockchain demystified ...", *cit.*, p. 74 y EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 45.

¹⁰²² "What is mining?". (Sin fecha). Disponible en: <https://www.coinbase.com/es/learn/crypto-basics/what-is-mining> (fecha de consulta: 1 de julio de 2022).

¹⁰²³ SCHELLEKENS, M. (2020). "Conceptualizations of the...", *cit.*, punto 44.

¹⁰²⁴ CNIL. (2018). *Solutions for...*, *Op. Cit.*, p. 2.

¹⁰²⁵ CZARNECKI, J. (2018). "Who is the data controller in a blockchain?". Disponible en: <https://newtech.law/en/who-is-the-data-controller-in-a-blockchain/> (fecha de consulta: 7 de julio de 2022).

un servidor de correo electrónico, pues este no es responsable legalmente por el contenido de los datos contenidos en el cuerpo del mensaje¹⁰²⁶.

3. Nodos

Un nodo es un punto de conexión virtual o físico, en el que se puede crear, recibir o transmitir un mensaje¹⁰²⁷. En Blockchain un nodo es un ordenador conectado a la red, que almacenan una copia de la cadena y ejecuta el *software* de funcionamiento¹⁰²⁸, cada nodo que se conectan a la Blockchain intercambia información con el resto de nodos sin necesidad de un intermediario.

Existen varias clases de nodos, los cuales se determinan de acuerdo a sus funciones y a apoyo a la red. Por ejemplo, en la cadena de bloques pública de bitcoin podemos destacar los usuarios que ejecutan los nodos ligeros y los nodos completos. Un nodo ligero es aquel que depende de los nodos completos para validar las transacciones¹⁰²⁹. Señala BUOCZ y otros que “Los usuarios que ejecutan nodos ligeros pueden crear transferencias para mover *BTC* de una dirección a otra. Los usuarios determinan directamente solo la dirección de entrada, la dirección de salida y la cantidad transferida de *BTC*”¹⁰³⁰. Este tipo de nodo no descargan la cadena de bloques de forma completa, sino que solo almacenan la cabecera de los bloques, es decir, que no conservan una copia del historial de transacciones, sino, la marca de tiempo, esto es, el número del bloque, la ubicación y el *hash* del bloque anterior. Mientras que, los nodos completos son los encargados de dotar seguridad a la red, aceptan transacciones y bloques de otros nodos completos, que validan y transmiten a otros nodos completos¹⁰³¹. También son los responsables de verificar que las transacciones, y que los bloques, cumplan con las reglas

¹⁰²⁶ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...., Op. Cit.*, p. 46.

¹⁰²⁷ “¿Qué son los nodos?” (2018). Disponible en: <https://academy.binance.com/es/articles/what-are-nodes> (fecha de consulta: 12 de julio de 2022).

¹⁰²⁸ “¿Qué es un nodo?” (2022). Disponible en: <https://academy.bit2me.com/que-es-un-nodo/> (fecha de consulta: 24 de julio de 2022).

¹⁰²⁹ “¿Qué es un nodo Bitcoin?” (Sin fecha). Disponible en: <https://www.bitpanda.com/academy/es/lecciones/que-es-un-nodo-bitcoin/#que-es-un-nodo-de-luz> (fecha de consulta: 22 de julio de 2022).

¹⁰³⁰ BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). “Bitcoin and the...”, *cit.*, p. 194.

¹⁰³¹ “Support the Bitcoin network by running your own full node”. (Sin fecha). Disponible en: <https://bitcoin.org/en/full-node#what-is-a-full-node> (fecha de consulta: 24 de julio de 2022).

de consenso, por ejemplo, verificar que se evite el doble gasto. Si no se cumplen estas reglas, cada nodo rechazará si no se ajusta a las reglas.

Para la Agencia Francesa de Protección de datos, los participantes que tienen derecho a escribir en una Blockchain y que deciden enviar datos para su validación (si estas labores se llevan a cabo en el marco de una actividad profesional, por cuenta de otra persona) si pueden ser considerados como responsables del tratamiento (mientras que si actúan a título personal caen dentro de la excepción del hogar y no se pueden considerar responsable)¹⁰³². De manera similar, otros autores también señalan que los nodos ligeros (usuarios) sean considerados como responsables del tratamiento, por ejemplo, FINK, argumenta que en una transacción de *BTC* el usuario es responsable del tratamiento de los datos de la parte a quien le está comprando o vendiendo la moneda, ya que estos definen el fin, (la compra o venta de *BTC*) y los medios (uso de la tecnología Blockchain) del procesamiento¹⁰³³. Asimismo, BARTHOLDY¹⁰³⁴ señala que, el usuario también puede ser el responsable del tratamiento, si este procesa datos personales de otras personas. De igual forma, READ y PEHLIVAN¹⁰³⁵, consideran que, si los nodos participan en la validación y creación de bloques, deben ser considerados como responsables del tratamiento. En esta misma línea, BACON¹⁰³⁶ y otros, señalan que cuando los usuarios envían sus transacciones, están ingresando datos personales en la cadena, por lo tanto, cada usuario, determina los fines del tratamiento al registrar una transacción y establecen los medios, al emplear Blockchain para ejecutar la transacción.

Sin embargo, aunque mayoritariamente se considere a los usuarios como responsables del tratamiento, BUOCZ y otros indican que los usuarios que ejecutan nodos completos y nodos ligeros no determinan los fines ni los medios del tratamiento, pues estos llevan a cabo sus actividades de acuerdo al protocolo de consenso, que no pueden modificar. Continúan señalando los autores que, estos usuarios solo deciden si se crea una transferencia, a quién va dirigida y cuánto *BTC* se transfiere, por lo que la finalidad

¹⁰³² CNIL. (2018). *Solutions for...*, *Op. Cit.*, pp. 1-2.

¹⁰³³ EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain...*, *Op. Cit.*, p. 48.

¹⁰³⁴ BARTHOLDY, M. (2021). "Responsibility for data on blockchains". Disponible en: <https://www.patrade.com/knowledge/responsibility-for-data-on-blockchains> (fecha de consulta: 23 de julio de 2022).

¹⁰³⁵ READ, I. I., & PEHLIVAN, C. N. (2020). "Blockchain and Data...", *cit.*, p. 43.

¹⁰³⁶ BACON, J., MICHELS, J. D., MILLARD, C., & SINGH, J. (2018). "Blockchain demystified ...", *cit.*, p. 64.

siempre será la transferencia de bitcoins y esto no puede ser cambiado por los nodos, así como tampoco tienen control sobre el tiempo durante el cual se almacenan los datos, los terceros que tienen acceso a esa información (recordemos que es público), así como tampoco los datos que se procesan, por lo que concluyen que, categorizar a los usuarios como responsables del tratamiento es una interpretación excesiva de la figura del responsable¹⁰³⁷. Consideramos más acertada esta tesis, puesto que la designación de los usuarios que ejecutan al tiempo el *software* de funcionamiento de una cadena de bloques, como responsables del tratamiento, no solo por los argumentos acertados antes esbozados, sino también, por el hecho de que en la práctica un usuario individualmente no puede asumir las obligaciones que conlleva tal designación, como por ejemplo, hacer cumplir el derecho al olvido o de rectificación, por lo que, sería inviable que los interesados puedan ejercer sus derechos. Por tanto, surge la cuestión si se pueden considerar a los usuarios que ejecutan nodos como corresponsables del tratamiento, pues estos como colectivo, sí que pueden realizar estas acciones.

3.1 Corresponsables del tratamiento

Hemos visto en el apartado anterior los actores principales que se pueden identificar en una cadena de bloques de carácter pública y distribuida, como puede ser, la criptomoneda de bitcoin. No obstante, no pudimos establecer claramente quién podría catalogarse como el responsable del tratamiento. Los desarrolladores de la plataforma y los mineros fueron descartados, ya que los primeros a pesar de que podría decirse que determinan el por qué, al diseñar la plataforma, no tratan datos personales. Los segundos, siguen el protocolo de consenso y no determinan el objeto de las transacciones, y los nodos, aunque hay una parte amplia de la doctrina que señalan a estos actores como responsables del tratamiento, esto en la práctica, individualmente hablando, no podrían cumplir con las obligaciones propias del responsable del tratamiento, Por ello surge el interrogante si ¿Podrían considerarse en su conjunto a los usuarios que ejecutan nodos en Blockchain como corresponsables del tratamiento?

Señala el Artículo 26. 1 del Reglamento General De Protección De Datos que “cuando dos o más responsables determinen conjuntamente los objetivos y los medios

¹⁰³⁷ BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). “Bitcoin and the...”, *cit.*, p. 165.

del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento”. De acuerdo a la jurisprudencia del Tribunal de Justicia de la Unión Europea, en su sentencia *Wirtschaftsakademie Schleswig-Holstein*¹⁰³⁸, se señaló que el administrador de una página de fans de Facebook podría considerarse corresponsable del tratamiento, ya que este al escoger esta red social le otorga a dicha empresa la posibilidad de colocar *cookies* en los ordenadores de cualquiera que visite su página de fans, por lo que le da la posibilidad a Facebook de tratar esos datos y, en consecuencia, el administrador contribuye al tratamiento de los datos personales de los visitantes de su página¹⁰³⁹. Hemos mencionado que los nodos completos no determinan los medios y el propósito del tratamiento, sin embargo, si tenemos en cuenta la interpretación amplia que da esta jurisprudencia podemos inferir los nodos juntos si pueden influir en la forma en cómo se tratan los datos en una Blockchain y convertirse en corresponsables del tratamiento.

Sin embargo, los usuarios que ejecutan nodos en Blockchain no determinan conjuntamente el por qué y el cómo del tratamiento¹⁰⁴⁰, tampoco determinan de mutuo acuerdo sus responsabilidades, ellos lo que hacen es descargar un *software*, instalar un nodo en un ordenador y registrarse por el protocolo preestablecido. De tal manera que no firman ningún acuerdo, sino que ingresan a un sistema regido por incentivos criptoeconómicos¹⁰⁴¹. Y aunque podríamos decir que esto no son requisitos para establecer la corresponsabilidad, sino más bien una obligación que se deriva, y que los nodos pueden cooperar (más del 51%) y de esta forma podrían ejercer las obligaciones que tienen frente a los interesados. No hay ningún incentivo económico (incentivo principal por el que cooperan) para que cumplan con las obligaciones establecidas en el RGPD, además identificar las personas que hay detrás de cada nodo no es sencillo dado que Blockchain es seudónimo¹⁰⁴², el interesado no tendría ante quien acudir pues hay

¹⁰³⁸ STJUE, Gran Sala, de 5 de junio de 2018, Asto: C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein y Wirtschaftsakademie Schleswig-Holstein GmbH/ Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht EU:C:2018:388, apartado 35. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210> (fecha de consulta: 29 de julio de 2022).

¹⁰³⁹ STJUE, Gran Sala, de 5 de junio de 2018, apartado 36.

¹⁰⁴⁰ MOEREL, L. (2019). “Blockchain and...”, *cit.*, p. 216.

¹⁰⁴¹ SCHELLEKENS, M. (2020). “Conceptualizations of the...”, *cit.*, punto 13.

¹⁰⁴² BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). “Bitcoin and the...”, *cit.*, p. 197.

ausencia de una figura central. Por tanto, aunque potencialmente podrían considerarse corresponsables del tratamiento, en la práctica fallan porque no es posible que cumplan con sus obligaciones.

3.2 Consideraciones acerca de los nodos

Es claro que identificar al responsable del tratamiento en una red pública y distribuida no es fácil, no solo porque los actores que potencialmente podrían considerarse como responsables no tienen la facultad para hacer cumplir el reglamento, sino que, el interesado ni siquiera tiene conocimiento ante quien acudir, en caso de que quiera ejercer sus derechos, pues los participantes se identifican mediante seudónimos. Nos encontramos con el dilema con que cualquiera que pueda incluir datos a la red podría calificar como responsable por los datos ingresados, y también es encargado del tratamiento, por la copia que tiene en su ordenador de la cadena de bloques. Podemos argumentar que en virtud de la cantidad de participantes que hay en una cadena de bloques, podríamos decir que estos, como un colectivo, podrían ser calificados como corresponsables. No obstante, esto en la realidad es poco factible que se dé, porque es administrativamente difícil de aplicar¹⁰⁴³. En resumen, no solo no podemos identificar al responsable del tratamiento en una cadena de bloques pública y distribuida y asignar responsabilidades, sino que, aun señalando a un colectivo como responsables, como pueden ser los nodos, estos no poseen un control efectivo sobre la cadena de bloques. Y no solo eso, sino que la identidad de los usuarios se desconoce, por lo que es poco probable que se realicen acuerdos de gobernanzas para distribuir sus responsabilidades. Desde luego, Blockchain como tecnología y habida cuenta la variedad de diseño, sí que puede haber proyectos que cumplan con el RGPD y que sea fácil la identificación del responsable, como puede ser, una Blockchain privada y autorizada. Por tal razón debe evaluarse cada caso concreto para determinar al responsable del tratamiento, pues no hay respuestas claras al respecto, ello se logrará a medida que el Comité Europeo de

¹⁰⁴³ THE SOVRIN FOUNDATION. (2020). *Innovation Meets Compliance Data Privacy Regulation and Distributed Ledger Technology*, Sorvin ORG. Disponible en: https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf (fecha de consulta: 29 de julio de 2022).

Protección de Datos, las agencias nacionales de protección de datos y los tribunales se pronuncien al respecto.

CONCLUSIONES

CONCLUSIONES

I. Blockchain y la ley.

- I. El 31 de octubre de 2008, en plena crisis financiera, Satoshi Nakamoto presentaba Bitcoin como un sistema de efectivo electrónico, totalmente *peer-to-peer*, que no requería la intervención de la banca, los gobiernos o bancos centrales para operar, sino de la criptografía. Surge como una forma de escape y protesta en contra de un sistema financiero manipulado y defectuoso, que dejó en evidencia los riesgos de la concentración de poder, y que la crisis financiera parecía reivindicar. Con Bitcoin nacería una nueva tecnología, Blockchain, cuyo uso iría más allá de las criptomonedas y las finanzas.
- II. Algunos de sus grandes atractivos son: por un lado, la accesibilidad, en la medida en que cualquier persona puede consultar la información en ella depositada. Por otro, el aroma libertario de los instrumentos gestionados directamente por los particulares de forma “anónima”, sin la mediación de las autoridades públicas ni de los grandes poderes económicos. Asimismo, pero no menos importante, la inmutabilidad y resistencia a manipulaciones de su registro. Paradójicamente, esas grandes características se convierten, a su vez, en su mayor hándicap, pues sus desafíos son en gran parte debido a estas particularidades.
- III. Al igual que internet en sus inicios, Blockchain se ha percibido como una tecnología imposible de regular, que permite la libertad de las personas al margen de cualquier estructura de control gubernamental. Sin embargo, internet al convertirse en un medio potencialmente lucrativo modificó su arquitectura técnica para permitir su regulación. Así, no les brindó a las personas la libertad que prometió, más bien se convirtió en un mecanismo para ejercer control y vigilancia sobre ellas, no solo por parte de los Estados, sino también por parte de las grandes corporaciones. Este parece ser el camino que está recorriendo Blockchain.
- IV. La cadena de bloques, junto con los contratos inteligentes, permiten impulsar cambios en el funcionamiento de la ley, lo que, teóricamente, permite emplear el código para regular el comportamiento de las personas. En este sentido, el código

no es la ley, sino que la ley se incorpora al código y este, a su vez, es controlado por los gobiernos y las grandes empresas.

V. La arquitectura técnica de la red determina lo que se puede hacer o no, a través del empleo de medios tecnológicos y materiales. A pesar de los beneficios en términos de eficiencia que puede representar emplear el código para regular la sociedad, existen riesgos, como la posibilidad de mayor vigilancia y control sobre el usuario, o la falta de transparencia de los procesos de regulación. En este sentido, las personas perciben esta regulación como algo natural, inherente al funcionamiento de la tecnología, sin tener conocimiento de cómo las empresas y los gobiernos controlan su comportamiento. Asimismo, y a pesar de la teórica democratización de la cadena de bloques, realmente encontramos una ausencia de procesos democráticos propios de la regulación tradicional, lo cual es indeseable para el estado de derecho.

VI. La tecnología Blockchain, permite a las personas, mediante el empleo de Smart Contracts, crear sus propios marcos regulatorios privados, que la doctrina ha nombrado como *lex criptografía*. Esto, teóricamente, permite a los individuos organizarse de forma descentralizada e independiente de cualquier autoridad gubernamental.

La *lex criptografía* ha sido valorada por algunos como una nueva *lex mercatoria*. Sin embargo, consideramos que no reemplazará al sistema legal tradicional, dado que no aporta un beneficio sustancial respecto a los sistemas ya existentes. En este sentido, que sea nuevo no significa que sea mejor, más aún si el código puede presentar errores y producir consecuencias materiales irreversibles. Si bien el Estado de derecho no es perfecto, no es tan ineficiente para que deba ser reemplazado por un gobierno del código informático, que no cuenta con ningún tipo de garantías democráticas, éticas ni constitucionales.

VII. A pesar de los desafíos que representan algunas de las características de Blockchain para su regulación, es una tecnología regulable. En primer lugar, la operación de la cadena de bloques (desarrolladores de *hardware*) y su adopción en masa (plataformas de intercambio de criptoactivos), requiere de la presencia de intermediarios. En los últimos años, hemos sido testigos del surgimiento de

nuevos actores en este sistema, así como de la formación de grandes empresas hegemónicas. Los intermediarios actúan como un punto de control, que permite aterrizar la descentralización sobre una jurisdicción concreta. De tal manera, los intermediarios constituyen uno de los principales objetivos de la intervención reguladora. Independientemente a esto, los reguladores además poseen las 4 modalidades de regulación (normas, arquitectura, ley y mercado) planteadas por Lessig, para someter la tecnología Blockchain a su régimen jurídico.

II. Blockchain y los contratos inteligentes

VIII. Los Smart Contracts representan una de las innovaciones más interesantes que ha traído consigo la tecnología Blockchain, no obstante, sus supuestos beneficios han sido exagerados. Su desarrollo es anterior a Bitcoin. De hecho, su origen se remonta al Intercambio Electrónico de Datos (1948). A pesar de ello, no fue hasta la década de los noventa que el criptógrafo NICK SZABO teorizó este concepto por primera vez. Sin embargo, debido a la incapacidad del sistema financiero y de la tecnología disponible en la época, no fue posible su puesta en práctica. Fue gracias al despliegue de Bitcoin y de Ethereum lo que hizo que pasaran de ser un mero concepto teórico a una realidad.

IX. Los contratos inteligentes son un término impreciso para un *software* que se ejecuta automáticamente. La partícula “contrato” puede ser engañosa, porque no necesariamente este va a tener relevancia jurídica. Es por ello que, estrictamente hablando, un mejor término sería “contratos legales inteligentes”. De igual forma, cabe destacar que la expresión “inteligente”, es asimismo errónea, pues, debido a su carácter determinista, los Smart Contracts siguen de forma ciega las instrucciones pre-programadas en su código.

X. Respecto a la consideración del Smart Contract como un contrato legal, cabe destacar que características como la descentralización, la inmutabilidad y seudonimato, unido a que el acuerdo esté expresado en lenguaje de programación, pueden ser un obstáculo para su relevancia jurídica.

En la legislación española, conforme al principio de libertad de forma, un acuerdo de voluntades puede expresarse en código informático. Sin embargo, este debe reunir los requisitos esenciales para ser considerado como válido, a saber,

consentimiento, objeto y causa. Estos dos últimos requisitos no suponen un problema por parte de los contratos inteligentes, no obstante, la aplicación del consentimiento es conflictivo. De tal manera, cuando el contrato se ejecuta y desarrolla en una Blockchain de carácter público, el seudonimato de las transacciones no nos permite constatar la capacidad de las partes. Lo que significa que, no podemos generalizar y afirmar que los contratos inteligentes no reúnen estos requisitos esenciales, pues existen diferentes tipologías, como tampoco se puede asegurar que todo contrato inteligente es un acuerdo legal. Por esta razón, habría que analizar cada caso concreto, para establecer si se trata o no de un contrato jurídicamente vinculante.

XI. Las limitaciones de los acuerdos en código no son solo jurídicas, sino también técnicas. Los Smart Contracts son programas informáticos, por lo que funcionan con Lógica Booleana, un concepto matemático que solo admite dos variables: “verdadero” o “falso” “1” o “0”. Por ello, no es posible la codificación de cláusulas ambiguas. Dicha inflexibilidad comporta una serie de costos *ex antes*. Las partes deben prever todas las circunstancias futuras, un objetivo poco realista, pues existen factores externos que no se pueden predecir, tal y como reconoce el derecho contractual tradicional, que corrige estas fallas de forma posterior.

XII. Contrariamente a lo que se ha promocionado, los contratos inteligentes no reducen los costos de transacción. Por un lado, para formar acuerdos completos, las partes deben aprender mucho sobre el mundo que les rodea. Por otro lado, las tarifas para ejecutar un acuerdo en una plataforma como Ethereum son prohibitivamente altas. Finalmente, el proceso de traducir cláusulas de lenguaje natural a lenguaje de programación es costoso, requiriendo de la presencia tanto de un especialista en leyes como de otro en programación. De tal manera, que los costos que deben asumir las partes son más altos que en la contratación tradicional. Lo que nos hace pensar si las famosas ganancias de eficiencia superan los costos que debemos asumir.

XIII. A pesar de la plétora publicitaria acerca del potencial de la contratación inteligente y su llamado a redefinir los sistemas clásicos de contratación, consideramos que, por ahora, solo los acuerdos más básicos podrían ser

íntegramente desarrollados y ejecutados en código. Es probable que las versiones exitosas que veamos de contratos inteligentes sean acuerdos híbridos, en el cual haya una pieza escrita en lenguaje natural y otra en código informático. En los contratos híbridos solo podrían automatizarse las obligaciones que se pueden expresar en código, como, por ejemplo, una cláusula de pago. De esta forma, el código sería una herramienta de apoyo para garantizar la ejecución de obligaciones susceptibles de programación, y no el contrato per se. Así, los términos contractuales escritos en lenguaje natural serían el contrato propiamente dicho. En consecuencia, la combinación de lenguaje natural y código aporta a la contratación los beneficios de la utilización de cada tipo: la flexibilidad del lenguaje natural y la ejecución automática y a prueba de manipulaciones del código.

XIV. Para que los contratos inteligentes se ejecuten de forma segura en una cadena de bloques, consideramos que no solo es necesario que haya un contrato de papel de respaldo, sino que se debe estipular que la versión del lenguaje natural tendrá prioridad sobre el código, dado que la mayoría de los contratantes no comprenderán el lenguaje de programación. De igual forma, es primordial que exista la facultad de modificación de los términos contractuales, es decir, la mutabilidad. Esta característica debe ser codificada al momento de la redacción, pues si no se hace, no es posible hacerlo con posterioridad, dado que los contratos inteligentes no se pueden modificar o actualizar. En este sentido, para que los contratos inteligentes superen los desafíos legales, implica que estos abandonen sus características (mutabilidad y ejecución automática) o que recurran a los sistemas heredados que pretenden sustituir, lo que nos hace pensar la necesidad de su empleo.

XV. Al igual que cualquier aplicación o programa informático, los Smart Contracts pueden contener errores en su código, o puede que las partes deseen realizar algún cambio, o que exista algún hecho sobreviniente que produzca resultados no deseados. En efecto, los contratos inteligentes no eliminan el incumplimiento, pues aun cuando el contrato tiene asegurada su ejecución a través de la red de nodos, no se puede garantizar que el código represente fielmente la obligación,

que existan errores de programación o que el acuerdo sea blanco de piratería o la explotación de su código.

XVI. La responsabilidad del desarrollador de un contrato inteligente deberá ser de carácter subjetivo en caso de que la falla algorítmica sea imputable a este, pues su labor afectará la condición legal de las partes durante la vigencia del contrato.

Si existe incumplimiento de las obligaciones, ya sea por un error de codificación o por un ataque informático, el derecho contractual tradicional ofrece la posibilidad de que, dependiendo del caso concreto, el acuerdo se pueda rescindir o modificar. No obstante, dejar sin efecto o rectificar es complejo en los Smart Contracts, pues el código siempre se ejecutará según lo programado. De tal modo, si las partes no incluyeron una cláusula que lo permitiese (cuestión habitual, pues es difícil anticipar todas las posibilidades de incumplimiento) será un desafío modificar el contrato. Aun existiendo la posibilidad de modificación, si el incumplimiento es una consecuencia directa de un ataque o *exploit*, podría haber consecuencias materiales irreversibles. Si la inobservancia de lo estipulado en el acuerdo no puede ser atribuible a una de las partes, porque es consecuencia directa de un error de codificación, no podemos calificarlo como incumplimiento. En este sentido, la ley debe adaptarse a las nuevas realidades tecnológicas y en este contexto es necesario un marco jurídico apropiado que determine los derechos y obligaciones de las partes, asigne responsabilidades y se adapte a las fallas algorítmicas que pueden presentar los contratos inteligentes.

XVII. Pese a que se exalte con vehemencia que una de las mejores características de los Smart Contracts es que eliminan la ambigüedad, lo cierto es que los términos vagos e imprecisos no son un anatema en la contratación. De hecho, son una característica deseable y necesaria, que deriva de una realidad que se encuentra en constante cambio. De tal manera, los contratos son deliberadamente ambiguos para adaptarse a los cambios. En este sentido, la rigidez de los contratos inteligentes no representa una ventaja, sino más bien una limitación, pues estos no tienen la capacidad de ajustarse a nuevos escenarios. ¿A quién y cómo beneficia esta rigidez? En realidad, a nadie. En efecto, la inflexibilidad podría aislar al contrato del contexto social en el cual se desarrolla y limitar su adopción en masa. El derecho contractual es dinámico y flexible, y aunque ello pueda

conducir a diversas interpretaciones y, por tanto, abrir la entrada a las disputas, lo cierto es que estas características son su mayor fortaleza.

XVIII. Los lenguajes de programación son más limitados y precisos que los naturales. De tal manera, a la hora de programar un acuerdo legal, existirán límites a la hora de representar la diversidad del lenguaje común. El código de contrato inteligente en todo momento va a estar relacionado con el lenguaje natural, sin embargo, es probable que esto no se logre al existir grandes diferencias en cuanto al funcionamiento de ambos lenguajes.

XIX. Con el propósito de que las partes estén seguras de que lo codificado representa fielmente sus intenciones y no ocasione resultados indeseados, la doctrina ha propuesto que se valide la semántica legal del código o que se cree un lenguaje equivalente, legible a la vez por máquinas y humanos. Consideramos que, pese a los esfuerzos de la academia por superar los desafíos que supone representar conceptos ambiguos en la contratación inteligente, es una tarea innecesaria, pues el código no puede controlar el comportamiento humano. Si una parte no actúa de buena fe o no cumple con sus obligaciones, es y seguirá siendo un problema del mundo físico.

III. La protección de los consumidores de criptoactivos: retos regulatorios

XX. Los avances tecnológicos han cambiado la forma en la que consumimos, teniendo cada vez un mayor peso en nuestras vidas el consumo digital. Por ello es fundamental no solo conocer las potenciales ventajas que ofrece Blockchain, sino ser consciente de los riesgos que implica. Progresivamente, ha aumentado el número de usuarios que optan por la inversión en criptoactivos, una industria que supone muchos riesgos. Se trata de un mercado complejo, opaco y potencialmente manipulable, que se ha desarrollado sin un marco jurídico que garantice unas protecciones mínimas a los consumidores.

XXI. Cuando un usuario emplea a proveedores de criptoactivos, como una plataforma de intercambio o de custodia, realmente no está empleando una Blockchain, sino a un intermediario que le ofrece una experiencia e interfaz de usuario similar a la de un banco tradicional. De tal manera, el usuario no está disfrutando realmente

de los beneficios de esta tecnología, dado que, si bien el contenido de la cadena de bloques es teóricamente seguro, los intermediarios no lo son. Por tanto, el usuario se enfrenta a un doble problema: por un lado, opera en un escenario inseguro que no cuenta con unas salvaguardas mínimas de protección al consumidor y, por otro lado, no se beneficia de los hipotéticos beneficios que le podría aportar la tecnología Blockchain.

XXII. La adquisición y custodia de criptoactivos a través de intermediarios como son las casas de cambio y billeteras, introducen concentración de poder a un sistema que se precia por ser descentralizado. Paradójicamente, estos actores han permitido el acceso simple y en masa por parte del consumidor promedio a la criptoeconomía. Sin embargo, no tienen un régimen jurídico aplicable, de tal manera que operar con criptoactivos implica tomar una serie de riesgos como robos, piratería y estafas de inversión.

XXIII. La centralización de las plataformas de compra-venta y de custodia, actúan como un único punto de fallo, razón por la cual se han convertido en el objetivo de ataques criminales. Asimismo, los consumidores no cuentan con garantías mínimas como un fondo de garantías. Por tal motivo, en los últimos años hemos sido testigos de cómo varias plataformas de intercambio se han declarado en insolvencia y con ellas los ahorros de muchas personas, donde la única vía que queda es el sistema judicial.

XXIV. La arquitectura técnica de gran parte de las cadenas de bloques limita en su arquitectura los mecanismos de reversión en caso de que las transacciones sean fraudulentas, erróneas o accidentales. Se culpa y se responsabiliza a los usuarios en caso de errores. Algo extremadamente arriesgado, pues las garantías de protección con que cuentan los usuarios son mínimas o inexistentes.

Las cadenas de bloques públicas no son sistemas descentralizados y neutrales como pretenden presentarse al público. Por lo general, solo un grupo reducido de personas tienen la capacidad de realizar cambios sustanciales en su arquitectura técnica. Que estas redes se perciban como descentralizadas genera que se exima de responsabilidades y obligaciones a los que están a cargo. Y que, en última, los consumidores no sean conscientes y no perciban los riesgos que ello implica.

XXV. A nivel europeo, diferentes organismos supervisores, a través de múltiples advertencias y notificaciones, han intentado dar aviso a los consumidores acerca de los peligros que supone invertir en una tecnología no regulada. Sin embargo, estas advertencias no evitaron lo predecible. En este sentido, las instituciones europeas contemplaron expectantes como se cernía sobre ellos un problema cada vez mayor. Se reprocha que, hasta que los reguladores y supervisores no se dieron cuenta del riesgo que representan los criptoactivos, en concreto las *stablecoins* para el sistema financiero, no tomaron medidas firmes al respecto.

XXVI. España no cuenta con un régimen jurídico específico para la protección de los consumidores de criptoactivos. Aunque, la CNMV aprobó a comienzos de 2022 una Circular que regula las reglas aplicables a la actividad publicitaria de los criptoactivos que no tengan la consideración de activos financieros. Esta norma somete bajo su ámbito de aplicación a los *influencers*. Huelga decir que, las medidas introducidas en esta Circular, aunque son un acercamiento, no son suficientes para garantizar la protección de los consumidores. Consideramos que no es conveniente mantener esta regulación en una zona gris, pues esta tecnología posee características únicas que requiere de soluciones específicas. En este sentido, las respuestas regulatorias deben ser conjuntas, no solo a nivel europeo, sino global.

XXVII. Los esfuerzos regulatorios se han centrado en temas de prevención de blanqueo de capitales y financiación del terrorismo. A nivel nacional el Banco de España habilitó un registro para los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Sin embargo, la inscripción en él no significa que la plataforma que lo haga sea confiable para los consumidores, pues el Banco de España no supervisa los riesgos financieros o de seguridad de estas plataformas, pudiendo asimismo dar una sensación de falsa seguridad.

XXVIII. Con el propósito de brindar una respuesta integral y unificada al desafío regulatorio de los criptoactivos, a finales de 2020, la Comisión Europea presentó la propuesta de Reglamento relativo a los mercados de criptoactivos. Dicha propuesta busca unificar la legislación, evitar el arbitraje regulatorio y la actual

fragmentación del mercado al interior de la UE. En este sentido, una regulación uniforme y común a nivel europeo le aportaría seguridad jurídica no solo a los usuarios, sino también a aquellas empresas que desean establecerse en la Unión.

XXIX. La propuesta no regula a las cadenas de bloques per se, sino a los criptoactivos que no entran en la categoría de instrumentos financieros, como los Security Tokens, pues estos están regulados por MiFID II. Es decir, se regulan a los intermediarios. Se contemplan 3 categorías de criptoactivos: ficha referenciada a activo (ART), ficha de dinero electrónico (EMT) y ficha de servicio. Se establece un régimen específico, con unos requisitos especiales para las ART y EMT, debido a los riesgos que estos representan para los consumidores y para el sistema financiero. Es decir, que las *stablecoins*, se convierten en el principal objetivo de la intervención reguladora. Por su parte, las fichas de servicio estarán sujetas a la categoría general, que es más laxa, dado que sus riesgos son menores.

XXX. MiCA regula las actuaciones de los proveedores de servicios de criptoactivos y establece una lista de *números clausus* de los servicios y actividades que pueden considerarse como tal. El hecho de que sea una lista cerrada puede suponer que algunos proveedores que no se encuentren en ella eludan sus responsabilidades. Se les exige que para prestar sus servicios estén autorizados y constituidos como persona jurídica con domicilio social en un Estado miembro de la UE, actuando la autorización como un pasaporte europeo.

XXXI. MiCA introduce medidas importantes para proteger a los consumidores frente a los riesgos a los que han sido expuestos por la ausencia de regulación. En concreto, se exige a los emisores y los proveedores de servicios de criptoactivos actuar de forma honesta, imparcial y profesional, advertir a los consumidores de los riesgos de pérdidas, contar con un pasaporte que les autorice prestar sus servicios, entre otros. Además, a los proveedores de servicios de criptoactivos se les exige, en concreto, el cumplimiento de requisitos prudenciales y administrativos. Asimismo, deberán contar con fondos propios y la adquisición de una póliza de seguro válida en toda la UE. Aunque se critica que el alcance de esta póliza no cubra la pérdida de dinero, robos y pirateos.

XXXII. Una de las salvaguardas más importante de la propuesta es que responsabiliza, a las plataformas de intercambio de criptoactivos y de custodia, en caso de que haya pérdida de dinero, robos o pirateos. La exigencia de esta política busca garantizar que el proveedor de servicios de criptoactivos no pueda perderlos debido a fraudes o negligencias. En este sentido, MiCA viene a poner coto a una de las principales causas por la cual los consumidores pierden su dinero.

XXXIII. El derecho de desistimiento es uno de los derechos más importantes que les otorga MiCA a los consumidores, aunque solo está previsto para las fichas de servicios, cuando no hayan sido admitidas a negociación en una plataforma de negociación de criptoactivos. Es decir, no aplica en caso de reventa. Esta medida es entendible, porque si no el precio dependería de las fluctuaciones del mercado.

XXXIV. Se exige a todos los emisores de criptoactivos (ficha referenciada a activo, ficha de dinero electrónico y ficha de servicio) la emisión de un libro blanco. Sin embargo, los requisitos de su contenido y autorización difieren en cada categoría. El libro blanco de los emisores de fichas referenciadas a activos deberá estar aprobado por parte de la autoridad competente, mientras que para las fichas de dinero electrónico y ficha de servicio solo se les exige la notificación. A pesar de que el reglamento impone medidas más duras para las *stablecoins*, el deber de solo notificación para las fichas de dinero electrónico se da, porque estos emisores han debido de estar previamente autorizados como entidades de crédito o de dinero electrónico.

XXXV. Los emisores de criptoactivos y sus órganos de dirección serán responsables civilmente ante los clientes respecto a la información contenida en el libro blanco y en el resumen. Los consumidores pueden reclamar daños y perjuicios, no obstante, tienen la carga de la prueba para demostrar que el emisor ha incumplido los requisitos de información. Consideramos que esta medida es injusta para los consumidores. Los emisores están en una mejor posición para tener el *onus probandi*, más aún, si tenemos en cuenta la complejidad técnica de los productos financieros y de la tecnología.

XXXVI. Se establecen una serie de requisitos para prevenir el abuso de mercado cuando los criptoactivos se sometan a una plataforma de negociación. Se hace especial énfasis en la posible manipulación del mercado, la comunicación ilícita y las operaciones con información privilegiada. Además, se asignan una serie de competencias a los diversos organismos públicos implicados. Uno de los principales objetivos de estas medidas es que las celebridades y los *influencers* sean más transparente en relación con los criptoactivos que promueven. Esta es una de las medidas más importante, habida cuenta que los mercados de criptoactivos son vulnerables a las prácticas de manipulación por la volatilidad de sus precios, que muchas veces es consecuencia de declaraciones o acciones de actores con reconocimiento público. Así que una vez que el reglamento entre en vigencia, se lo pensarán dos veces antes de intentar promocionar de forma encubierta estos productos o de hacer aseveraciones sobre los mismos.

XXXVII. MiCA no ha estado exenta de críticas. No solo por la burocracia, que puede llegar a ser un factor limitante para el acceso al mercado de compañías emergentes, con pocos recursos o que no estén ya posicionadas a nivel europeo, acentuando aún más el riesgo de centralización y reduciendo la tan necesaria competitividad del mercado. También porque para algunos, paradójicamente, no sea suficiente para la protección a los consumidores, o porque no se aborden desarrollos como los NFTs y DeFi, para lo cual, tengamos que esperar a MiCA II. En este sentido, consideramos que, si bien puede que no sea un marco regulatorio completo y que llega un poco tarde, si es un paso hacia la dirección correcta, más aún, si tenemos en cuenta el ritmo de avance de esta tecnología y de las consecuencias indeseables que ha traído consigo la ausencia de regulación. La pérdida de dinero, las estafas, y los robos de los cuales han sido víctimas millones de personas es lo que obtenemos cuando permitimos que un grupo reducido de programadores de código y de empresas tecnológicas modelen nuestro modo de vida. Los consumidores deben contar con medidas mínimas que garanticen sus derechos, independientemente si se emplea una Blockchain o no. En este sentido, es claro que la regulación debe ser tecnológicamente neutral. Esta tecnología se debe someter al estado derecho, ninguna innovación debería estar por encima de este.

IV. Blockchain y resolución de disputas descentralizada

XXXVIII. Si bien la ejecución automática dota al contrato de eficiencia, esta no elimina las controversias en la contratación inteligente, sobre todo si consideramos la complejidad técnica y el entorno lucrativo en el cual se desarrolla esta tecnología. La justicia tradicional tiene la capacidad de resolver disputas transfronterizas, no obstante, debido a características como el seudonimato y la inmutabilidad, este sistema se ha percibido como inadecuado e inaccesible. Con la finalidad de preservar las características de Blockchain, desde el entorno de la propia tecnología han emergido varias plataformas de resolución de disputas adaptadas a los escenarios disruptivos y libertarios de las cadenas de bloques.

XXXIX. Las plataformas de resolución de disputas que se han desarrollado en el entorno Blockchain son una evolución de los sistemas ODR que surgieron como respuesta al auge de las controversias de escaso valor del comercio electrónico. Las plataformas Blockchain están especializadas en resolver disputas entre partes no identificadas, mediante un procedimiento simplificado y binario, que cuenta con varias características comunes. Estas son la sabiduría de las multitudes, la teoría de juegos (actúa como un método para prevenir la corrupción e incentivar económicamente a los jurados o árbitros), *Crowdsourced* y el arbitraje.

XL. Los sistemas CODR aportan eficiencia, descentralización y rapidez. Si bien estas características conservan los ideales de la tecnología, siendo bienvenidos y celebrados por sus defensores, lo cierto es que están llenos de incertidumbre. En primer lugar, los jurados no poseen conocimientos especializados sobre la materia del conflicto, la selección de los mismos se hace de forma aleatoria y, aunque existan barreras económicas de entrada, estas medidas pueden no ser suficientes para impedir el ingreso de usuarios inexpertos. Asimismo, el empleo de la teoría de juegos para impartir justicia genera dudas en relación a si es adecuada para que los miembros del jurado converjan en la decisión más justa, más aún, si tomamos en consideración que no hay comunicación ni deliberación entre ellos, y al hecho de que toman su decisión guiados por sus propios intereses económicos (no se inclinan por lo que consideren más equitativo o más justo, sino en una predicción de la decisión de sus compañeros).

En este sentido, la sabiduría de las multitudes no necesariamente va a generar la decisión más justa, pues los grupos en ocasiones pueden tomar decisiones equivocadas, como lo demuestran las burbujas. Igualmente, los mecanismos CODR no permiten soluciones “salomónicas” pues los procesos suelen ser binarios y los árbitros deben decidir sobre dos respuestas predeterminadas. De manera que, consideramos que la teoría de juegos no es mejor que las estructuras legales tradicionales.

XL I. Otros proyectos emplean el arbitraje para la resolución de conflictos en el entorno de las cadenas de bloques. Este mecanismo es atractivo para este ecosistema, debido a que las partes pueden elegir árbitros especializados en Blockchain y con experiencia, con posibilidad de ejecución casi global. Estos atributos se adaptan mejor que la justicia tradicional a las circunstancias singulares de la tecnología Blockchain.

XL II. Las reglas de CNUDMI son tecnológicamente neutral en su aplicación del comercio electrónico, por lo que pueden emplearse aquí también. Sin embargo, hay motivos de preocupación respecto a la validez, y costos de los procedimientos llevados a cabo por estas plataformas. Hay incertidumbre respecto a la validez de la cláusula compromisoria, si esta está redactada en lenguaje de programación. Si bien podría considerarse válida si se hace una interpretación amplia de la Ley Modelo y la Convención sobre comunicaciones electrónicas, una interpretación restrictiva puede negarle su validez en algunos Estados. Una forma de evitar esta incertidumbre es tener una copia del contrato en lenguaje natural, algo paradójico, dado que, de nuevo, el Smart contract requiere de los sistemas tradicionales para completarse.

XL III. En cuanto al reconocimiento y ejecución, la presentación auténtica y original del laudo podría certificarse en la misma cadena de bloques, pues la red es a prueba de manipulaciones y es de acceso público. Si la decisión se puede codificar en lenguaje de programación, su cumplimiento estará garantizado por el código, por lo que no habrá necesidad de solicitar la ejecución en sede judicial. En caso contrario, si el laudo afecta hechos que suceden por fuera de Blockchain, el

reconocimiento por vía judicial supone una movilización de recursos, que en muchos casos puede llegar a ser mayor que el valor económico de la disputa.

XLIV. A día de hoy, CODR puede ser la opción más conveniente para resolver disputas de escaso valor en el ecosistema Blockchain, a pesar de que no sea la opción más justa, puede que sea la única para partes no identificadas. Estas plataformas tienen mucho potencial, sin embargo, es necesario una respuesta regulatoria global que establezca estándares mínimos de justicia, equidad procesal y debido proceso.

XLV. Para controversias más complejas que requieran cierto nivel de especialización, el arbitraje parece ser la mejor alternativa, aunque sea necesario un contrato tradicional de respaldo y para su reconocimiento y ejecución se requiera de la identificación de las partes, lo que también implica que estas se sometan a instituciones tradicionales y centralizadas. Si los contratantes aspiran tener seguridad sobre un resultado justo y razonable, esas garantías solo las pueden hallar a través de los procedimientos de la ley y no por fuera de ella. Así lo han entendido las plataformas que pretenden que sus laudos sean legalmente vinculantes.

V. Blockchain y el Reglamento General De Protección De Datos

XLVI. El RGPD es una norma tecnológicamente agnóstica, por lo que su aplicación no está pensada para ninguna tecnología en específico. Sin embargo, entra en tensión con varias de las características de Blockchain. El ámbito de aplicación se circunscribe a los datos personales, excluyendo de su alcance los datos anónimos. Además, el concepto de dato personal conforme a lo establecido en el Reglamento es bastante amplio, por lo que, si tenemos en cuenta los avances tecnológicos, puede que un dato al momento de su recolección se considere anónimo, pero con el paso del tiempo se convierta en dato personal. En este marco, lograr la anonimización de un dato se torna complejo. Cualquier información va a estar relacionada con una persona identificada e identificable, máxime si tenemos en cuenta no solo el progreso tecnológico, sino el desarrollo de procesos como el análisis de datos, los incentivos económicos y la facilidad de hallar información

sobre millones de personas gracias a la omnipresencia de dispositivos inteligentes conectados a internet.

XLVII. Se ha discutido si las dos soluciones criptográficas que emplea Blockchain (función *hash* y la criptografía asimétrica o clave pública) son o no datos personales.

Una transacción en Blockchain representa una interacción entre dos partes, aunque su empleo puede variar de una cadena de bloques a otra. Una transacción puede transmitir criptomonedas, pero también se pueden emplear para registrar datos notariales, diplomas, historiales médicos, etc. Estos datos se encuentran en la carga útil y se conocen como datos transaccionales. Por lo general se almacenan de forma cifrada o mediante *hash*.

La función *hash* no se considera como una técnica de anonimización por sí misma, aunque en determinadas circunstancias, en la que se apliquen técnicas adicionales, sí que puede llegar anonimizar datos personales. Habrá que evaluar si el riesgo de reidentificación es probable, es decir, valorar los costes, el tiempo, la información en manos de tercero, la tecnología disponible y sus avances. Por lo tanto, las cadenas de bloques procesan datos personales, de modo que le es aplicable el Reglamento General de Protección de datos, aunque, este, aún continúa siendo un debate abierto.

XLVIII. La clave pública se utiliza para autenticar y ofuscar las identidades de los participantes. Los usuarios en lugar de identificarse con sus nombres lo hacen mediante una dirección. No hay dudas de que la criptografía asimétrica constituye un dato personal, pues al estar expuesta de forma pública se puede combinar con otro tipo de información, como, la dirección IP de los participantes, y lograr que estos se reidentifiquen de forma indirecta. Es más, la clave pública está asociada a otros identificadores únicos como son las cookies, firmas de dispositivo, entre otros, que son considerados datos personales. En este sentido, las identidades de los usuarios en una cadena de bloques no se hallan de forma anónima, sino seudónima, por lo tanto, están bajo el ámbito de aplicación del RGPD. Si bien la seudonimización reduce la vinculabilidad de los datos, sigue habiendo altas probabilidades de identificar a los interesados.

XLIX. El Reglamento asume que los datos pueden eliminarse o modificarse a petición del interesado. Es complejo conciliar el borrado de los datos con una tecnología que hace prohibitivamente alto eliminar o modificar la información almacenada, particularmente si de esta característica depende su integridad. El RGPD no define qué se entiende por supresión, así como tampoco hay una guía oficial que oriente sobre el particular. En este sentido, la observancia del derecho al olvido por parte de Blockchain depende de la interpretación que se haga de la supresión de datos. Una lectura estricta sugiere que se deben eliminar los datos, lo que en una cadena de bloques supone una bifurcación dura (que requiere la cooperación al menos la mitad de los nodos), sin embargo, esto aún no eliminaría los datos, pues dicha información aún seguirá existiendo en la Blockchain antigua. En contraste, una interpretación flexible y matizada puede permitir que para el cumplimiento de este derecho se prescinda del borrado material de los datos, en virtud de la imposibilidad técnica hacerlo en una tecnología de carácter inmutable, de modo que la supresión se lograría con obstaculizar o imposibilitar la divulgación de los datos. Sin embargo, a falta de un pronunciamiento oficial por parte del CEPD y del TJUE, hay incertidumbre sobre la interpretación que se le debe de dar. En ese orden de ideas, se hace patente la necesidad de una guía que se pronuncie claramente sobre el tema.

L. Para cumplir con el derecho al olvido se han sugerido varias soluciones técnicas, como, por ejemplo, almacenar los datos por fuera de Blockchain, la destrucción de las claves de cifrado, la mutabilidad de la cadena, la anonimización de los datos, la poda, entre otros, los cuales tienen sus ventajas e inconvenientes, tanto a nivel técnico, como jurídico. En este orden de ideas, no podemos generalizar y afirmar que el derecho al olvido es incompatible con Blockchain. No obstante, en redes de carácter público donde la inmutabilidad suele ser un punto inflexible e innegociable, no es posible la materialización de este derecho.

LI. El derecho de rectificación también entra en tensión con la inmutabilidad de Blockchain. Sin embargo, consideramos que tampoco es incompatible con esta tecnología. Lo mismo sucede con el principio de minimización de datos, que desafía la naturaleza acumulativa y replicada de Blockchain (cada nodo guarda una copia de la base de datos), así como con el principio de limitación del plazo

de conservación (puesto que los datos se procesan de forma permanente). Nuevamente, la respuesta depende de la arquitectura técnica de cada Blockchain, pues en una red pública como Bitcoin, la aplicación de estos principios no es posible.

LII. El RGPD concibe que la responsabilidad del tratamiento de los datos estará a cargo del responsable del tratamiento, ante quien los interesados ejercerán sus derechos. Sin embargo, no es posible identificarlo en una red de carácter público, situación que empeora debido a que los actores que podrían ser señalados como tales (nodos), no tienen un control efectivo sobre la cadena de bloques, de manera que no pueden dar cumplimiento con las obligaciones del Reglamento. Asimismo, los interesados no sabrían ante quién acudir para ejercer sus derechos, pues la identidad de los nodos se encuentra de forma seudónima.

LIII. Existen muchas variedades de cadenas de bloques, por ello no podemos generalizar y afirmar que esta tecnología no es compatible con los principios y derechos reconocidos por el RGPD. Lo que sí podemos asegurar, al menos a día de hoy, es que una Blockchain pública como Bitcoin o Ethereum no da cumplimiento con las disposiciones del Reglamento. No obstante, no podemos admitir que no hay nada que se pueda hacer. Los reguladores pueden imponer requisitos a los diseños de las cadenas de bloques para que estas cumplan con la ley y hacer ilegal el empleo de redes que no observen tales requisitos. Blockchain es una tecnología en continuo desarrollo, por lo que no podemos dar nada por sentado.

LIV. Con el estado actual de la tecnología Blockchain, consideramos que una red pública no protege la privacidad de sus usuarios, pues toda la información es transparente, pública y disponible, con el objetivo de que cualquier persona pueda visualizar y verificar su contenido. De hecho, ese es su objetivo y la clave de su integridad. Evidentemente, habrá situaciones en que la transparencia y la publicidad pueden llegar a ser deseables, pero, definitivamente, creemos que poner datos financieros o de salud de forma pública y al alcance de todos no parece ser una buena idea, más aún, si esos datos no se pueden eliminar o modificar. En este sentido, consideramos que una Blockchain no protege la

privacidad de las personas, de hecho, es menos privado que la banca tradicional, pues esta está sometida a unos estándares mínimos de privacidad. La regulación es necesaria, pues solamente así los usuarios pueden tener garantías básicas de seguridad.

Reflexiones finales

LV. Probablemente, el rechazo a nuestras entidades de crédito tradicionales, así como de nuestros Estados, han llevado en gran parte al surgimiento descontrolado de esta tecnología. No podemos menospreciar el sueño de SATOSHI, de hecho, sus ideales son dignos de perdurar en nuestra sociedad. Si bien es cierto que el sistema financiero actual cuenta con un gran número de fallos, los consumidores son conscientes de ellos y, en la medida de lo posible, han desarrollado una capacidad de crítica a los mismos. Sin embargo, existe la sensación de que, ocultándose tras una serie de ideales libertarios, gran parte de la población ha caído en un sistema mucho más centralizado, corrupto y con menos garantías de lo que teníamos previamente.

A lo largo de nuestro trabajo de investigación hemos mencionado distintas causas por las cuales Blockchain surgió como la tecnología llamada a cambiar el mundo, y como, asimismo, esta ha ido poco a poco “traicionando sus propios ideales” hasta devenir en lo que se ha convertido hoy día. Véase, en un mundo donde la población duda del Estado que la controla y le pone límites (acrecentada con la pandemia de la COVID-19), de una Banca que especula con su dinero y de una serie de grandes corporaciones que manipula a sus usuarios a través de sus datos personales, logrando modificar sus hábitos de consumo.

En uno de los puntos más recóndito de internet surge una tecnología barata, descentralizada, anónima, y a prueba de manipulaciones que, teóricamente, les permitiría a las personas lograr una mayor libertad. Se transmite que el Estado ni nadie podrá interferir en ella, que será una tecnología democrática, por y para el usuario, en la cual seremos completamente anónimos. No obstante, si ahondamos en los hechos, más allá de la exageración y analizamos con crítica estas supuestas características, encontramos que estas afirmaciones son engañosas. No es una tecnología descentralizada, anónima o barata. Blockchain no elimina a los

intermediarios, los cambia. En este sentido, es fundamental que los reguladores comprendan esta realidad.

Asimismo, y más allá del componente idealista, gran parte de la aceptación que ha recibido por parte de la población promedio se debe a la posibilidad de hacerse rico de la noche a la mañana, en un mundo desesperado por una pandemia. Sin embargo, esta burbuja ya empieza a mostrar los primeros signos de resquebrajarse, huelga decir, que las criptomonedas perdieron el 65% de su valor a lo largo del 2022. Finalmente, cabe plantearse hasta qué punto un usuario promedio entiende esta tecnología y, debido a ello, hasta qué punto este mismo usuario posee libertad, al estar jugando a un juego del cual siquiera conoce las reglas. Tal y como se ha arraigado en el conocimiento popular, no podemos más que repetir la célebre cita “aquel que no conoce su historia, está condenado a repetirla”.

No le debemos tener miedo a los desafíos, no obstante, la respuesta a esos desafíos solo los podemos encontrar en la ley y nunca en el código.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

- ABEDI, F., ZELEZNIKOW, J. & BRIEN, C. (2019). “Developing regulatory standards for the concept of security in online dispute resolution systems”, *Computer Law & Security Review*, Vol. 35, No. 5. Disponible en: <http://www.sciencedirect.com/science/article/pii/S026736491830390X> (fecha de consulta: 18 de diciembre de 2020).
- ACAR, G. (2018). “Four cents to deanonymize: Companies reverse hashed email addresses”. Disponible en: <https://freedom--to--tinker-com.translate.goog/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/? x tr sl=en& x tr tl=es& x tr hl=es& x tr pto=op> (fecha de consulta: 7 de agosto de 2021).
- ACKERMANN, R. (2022). “Ethereum abandona la criptomoneda y adopta la prueba de participación”, *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/14589/ethereum-abandona-la-criptomoneda-y-adopta-la-prueba-de-participacion> (fecha de consulta: 23 de noviembre de 2022).
- ADLERSTEIN, D. (2017). “Are Smart Contracts Smart? A Critical Look at Basic Blockchain Questions”. Disponible en: <https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract> (fecha de consulta: 16 de marzo de 2020).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2022). “Derecho de supresión ("al olvido"): buscadores de internet”. Disponible en: [https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=el%20derecho%20de%20supresi%c3%b3n%20\('pertinencia%20previstos%20en%20la%20normativa](https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=el%20derecho%20de%20supresi%c3%b3n%20('pertinencia%20previstos%20en%20la%20normativa) (fecha de consulta: 1 de junio de 2022).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021). “Cifrado y Privacidad (V): la clave como dato personal”. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-la-clave-como-dato-personal> (fecha de consulta: 20 de enero de 2022).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2021). *10 malentendidos relacionados con la anonimización*. Disponible en: <https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf> (fecha de consulta: 2 de agosto de 2021).

- AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2018). *Manual de legislación europea en materia de protección de datos*. Disponible en: <https://fra.europa.eu/es/publication/2020/manual-de-legislacion-europea-en-materia-de-proteccion-de-datos-edicion-de-2018> (fecha de consulta: 1 de junio de 2021).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2019). *Introducción al hash como técnica de seudonimización de datos personales*. Disponible en: <https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf> (18 (fecha de consulta: 2 de octubre de 2021).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Disponible en: <https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf> (fecha de consulta: 20 de junio de 2021).
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2010). “Blockchain (II): Conceptos básicos desde la protección de datos”. Disponible en: <https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos> (fecha de consulta: 16 de agosto de 2021).
- AKHTARUZZAMAN, M., BOUBAKER, S., NGUYEN, D. K., & RAHMAN, M. (2022). “Systemic risk-sharing framework of cryptocurrencies in the COVID–19 crisis2. *Finance research letters*. Disponible en: https://www.sciencedirect.com/science/article/pii/S154461232200099X#cit_3 (fecha de consulta: 1 de septiembre de 2022).
- AL JAWAHERI, H., AL SABAH, M., BOSHMAF, Y., & ERBAD, A. (2020). “Deanonymizing Tor hidden service users through Bitcoin transactions analysis”, *Computers & Security*, Vol. 8. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404818309908> (fecha de consulta: 17 de enero de 2022).
- ALAG, A. & RAMPHUL, S. (Sin fecha). “Interaction between blockchain technology and arbitration”. Disponible en: <http://arbitration.mu/blockchain-arbitration/> (fecha de consulta: 5 de abril de 2021).

- AL KHALIL, F., CECI, M., O'BRIEN, L. & BUTLER, T. (2017). "A Solution for the Problems of Translation and Transparency in Smart Contracts". Disponible en: <https://tinyurl.com/y4mdetzk> (fecha de consulta: 6 de octubre de 2020).
- ALLEN, J. (2018). "Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Languages", *European Review of Contract Law*, Vol.14, No. 4, pp. 307-343. Disponible en: <https://doi.org/10.1515/ercl-2018-1023> (fecha de consulta: 12 de junio de 2020).
- ALLENDE, M. (2018). ¿Pública, federada o privada? Explora los distintos tipos de blockchain". Disponible en: <https://blogs.iadb.org/conocimiento-abierto/es/tipos-de-blockchain/> (fecha de consulta: 2 de diciembre de 2022).
- ALLEN, D., LANE, A. & POBLET, M. (2019). "The Governance of Blockchain Dispute Resolution", *Harvard Negotiation Law Review*, Vol. 25, pp. 75-101. Disponible en: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/haneg25&div=5&id=&page=> (fecha de consulta: 16 de agosto de 2019).
- ALVARES- CARO, M. (2016). "El derecho a la supresión o al olvido", *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, (Dirs. PIÑAR-MAÑAS, J.), Ed.: Reus, pp. 241-256.
- ANDREW, J., & BAKER, M. (2021). "The general data protection regulation in the age of surveillance capitalism, *Journal of Business Ethics*, Vol. 168, No. 3. Disponible en: <https://link.springer.com/article/10.1007/s10551-019-04239-z> (fecha de consulta: 3 de agosto de 2021).
- APARICIO, B. (2018). "Chapter 1: the challenges associated with smart contracts: formation, modification, and enforcement", *Smarts contracts: Is the Law Ready?* (Dirs. Smart Contracts Alliance & Chamber of Digital Commerce), pp. 14-35.
- APCPD. (2018). "Que es y quienes forman el Grupo de trabajo del articulo 29". Disponible en: <https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/> (fecha de consulta: 23 de abril de 2022).
- ARIAS-POU, M. (2016). "Definiciones a efectos del Reglamento General de Protección de Datos", *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, (Dirs. PIÑAR-MAÑAS, J), Ed.: Reus, pp. 115-134.

- ASOCIACIÓN DE FABRICANTES Y DISTRIBUIDORES. (Sin fecha). “¿Qué es el estándar GS1?”. Disponible en: <https://www.aecoc.es/generador-codigo-barras/#FAQS> (fecha de consulta: 17 de junio de 2020).
- ASOCIACIÓN PROFESIONAL DE CONSULTORES EN PROTECCIÓN DE DATOS. (2016). “Que es y quienes forman el Grupo de trabajo del artículo 29”. Disponible en: <https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/> (fecha de consulta: 17 de junio de 2021).
- ASPRIS, A., FOLEY, S., SVEC, J., & WANG, L. (2021). “Decentralized exchanges: The “wild west” of cryptocurrency trading”, *International Review of Financial Analysis*, Vol. 77. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S1057521921001782#fn0015> (fecha de consulta: 18 de agosto de 2022).
- AST, F. (2017). “El DAO: Breve Historia de la Primera Organización Descentralizada”. Disponible en: <https://medium.com/astec/el-dao-breve-historia-de-la-primera-organizaci%C3%B3n-descentralizada-e85980f99787> (fecha de consulta: 23 de diciembre de 2019).
- AST, F. (2017). “Kleros, a Decentralized Court System for the Internet (Abridged)” Disponible en: <https://link.medium.com/bWcrPDghdgb> (fecha de consulta: 16 de febrero de 2021).
- AST, F., & DEFFAINS, B. (2020). “When online dispute resolution meets blockchain: The birth of decentralized justice”, *Stanford Journal of Blockchain law & policy*, Vol. 4. Disponible en: <https://stanford-jblp.pubpub.org/pub/birth-of-decentralized-justice/release/1> (fecha de consulta: 22 de marzo de 2022).
- AST, F. & LESAEGE, C. (2019). “White Paper”, V. 1.0. 7. Disponible en: https://kleros.io/whitepaper_es.pdf (fecha de consulta: 16 de febrero de 2021).
- AST, F., & LESAEGE, C. (2019). “Kleros, a protocol for a Decentralized Justice System”, pp. 24. Disponible en: *Dispute Revolution: The Kleros Handbook of Decentralized Justice* Disponible en: <https://ipfs.kleros.io/ipfs/QmZeV32S2VoyUnqJsRRCh75F1fP2AeomVq2Ury2fTt9V4z/Dispute-Resolution-Kleros.pdf> (fecha de consulta: 20 de diciembre de 2020).

- ATENIESE, G., MAGRI, B., VENTURI, D., & ANDRADE, E. (2017) “Redactable blockchain—or—rewriting history in bitcoin and friends”, *2017 IEEE European symposium on security and privacy*, pp. 111-126. Disponible en: <https://ieeexplore.ieee.org/document/7961975> (fecha de consulta: 21 de junio de 2022).
- AUTORIDAD BANCARIA EUROPEA. (2021).” Crypto-assets: ESAs remind consumers about risks”. Disponible en: <https://www.eba.europa.eu/financial-innovation-and-fintech/publications-on-financial-innovation/crypto-assets-esas-remind-consumers-about-risks> (fecha de consulta: 8 de agosto de 2022).
- AUTORIDAD BANCARIA EUROPEA. (2013). “Aviso a los consumidores sobre las monedas virtuales”. Disponible en: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598420/00742a76-9c02-46c5-a615-40105fe75b94/EBA_2013_01030000_ES_TRA1_Vinay.pdf?retry=1 (fecha de consulta: 4 de agosto de 2022).
- AUTORIDAD EUROPEA DE VALORES Y MERCADOS, AUTORIDAD BANCARIA EUROPEA & AUTORIDAD EUROPEA DE SEGUROS Y PENSIONES DE JUBILACIÓN. (2022). “Los reguladores financieros de la UE advierten a los consumidores sobre los riesgos de los criptoactivos”. Disponible en: <https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/InformacionInteres/EBA/Arc/Fic/2022-03-14-notaconjuntaautoridadesUE-cripto.pdf> (fecha de consulta: 4 de agosto de 2022).
- AUTORIDAD EUROPEA DE VALORES Y MERCADOS, AUTORIDAD BANCARIA EUROPEA & AUTORIDAD EUROPEA DE SEGUROS Y PENSIONES DE JUBILACIÓN. (2018). “ESMA, ABE y AESPJ advierten a los consumidores de los riesgos de las monedas virtuales”. Disponible en: <https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/Noticias%20Ultima%20Hora/EBAVirtualCurrenciesES.pdf> ((fecha de consulta: 4 de agosto de 2022).
- ATZEI, N., BARTOLETTI, M., & CIMOLI, T. (2017). “A survey of attacks on ethereum smart contracts sok”, *International conference on principles of security and trust*, pp. 164-186, Springer, Berlin. Disponible en: https://dl.acm.org/doi/10.1007/978-3-662-54455-6_8 (fecha de consulta: 10 de mayo de 2020).

- AVAST. (2022). “¿Qué son los keyloggers y cómo funcionan?” Disponible: <https://www.avast.com/es-es/c-keylogger> (fecha de consulta: 6 de febrero de 2023)
- BACON, J., MICHELS, J. D., MILLARD, C., & SINGH, J. (2018). “Blockchain demystified: a technical and legal introduction to distributed and centralized ledger”, *Richmond Journal of Law & Technology*, Vol. 25, No. 1. Disponible en: <https://jolt.richmond.edu/files/2018/11/Michelsetal-Final-1.pdf> (fecha de consulta: 27 de agosto de 2021).
- BAIR, T. (2019). “How Decentralized Tech Can End the Privacy Crisis in 2020”. Disponible en: <https://www.coindesk.com/how-decentralized-tech-can-end-the-privacy-crisis-in-2020> (fecha de consulta: 5 de enero de 2020).
- BANCO DE ESPAÑA (2022). *Informe de estabilidad financiera. Primavera 2022*. Disponible en: https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinanciera/22/IEF_Primavera2022.pdf (fecha de consulta: 11 de septiembre de 2022).
- BANCO DE ESPAÑA (2022). “Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos”. Disponible en: https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html (fecha de consulta: 21 de octubre de 2022).
- BANCO DE ESPAÑA. (2018).” Comunicado conjunto de la CNMV y del Banco de España sobre “criptomonedas” y “ofertas iniciales de criptomonedas” (ICOs)”. Disponible en: https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/pre_sbe2018_07.pdf (fecha de consulta: 4 de agosto de 2022).
- BANCO DE ESPAÑA, COMISIÓN NACIONAL DEL MERCADO DE VALORES & DIRECCIÓN GENERAL DE SEGUROS Y FONDOS DE PENSIONES (2022). “Comunicado conjunto del Banco de España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos”. Disponible en:

https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/22/pre_sbe2022_19.pdf (fecha de consulta: 4 de agosto de 2022).

BANCO DE ESPAÑA & COMISIÓN NACIONAL DEL MERCADO DE VALORES. (2021). “Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión”. Disponible en: <https://www.cnmv.es/portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D> (fecha de consulta: 4 de agosto de 2022).

BANSAL, R. (2019). “Enforceability of Awards from Blockchain Arbitrations in India”, *Kluwer Arbitration Blog*. Disponible en: <http://arbitrationblog.kluwerarbitration.com/2019/08/21/enforceability-of-awards-from-blockchain-arbitrations-in-india/> (fecha de consulta: 1 de febrero de 2021).

BARCELÓ, R. (2021). “El impacto de la tecnología blockchain en la contratación privada: ¿hacia una contratación inteligente?”, *Revista de los Estudios de Derecho y Ciencia Política*, No. 33, p. 4. Disponible en: <https://raco.cat/index.php/IDP/article/view/n33-barcelo/481692> (fecha de consulta: 17 de enero de 2023).

BARLOW, J. P. (2009). “Declaración de independencia del ciberespacio.” *Periférica Internacional. Revista para el análisis de la cultura y el territorio*, Vol. 1, No. 10, pp. 241-242. Disponible en: <https://revistas.uca.es/index.php/periferica/article/view/943> (fecha de consulta: 29 de septiembre de 2019).

BARTHOLDY, M. (2021). “Responsibility for data on blockchains”. Disponible en: <https://www.patrade.com/knowledge/responsibility-for-data-on-blockchains> (fecha de consulta: 23 de julio de 2022).

BARTOLETTI, M. & POMPIANU, L. (2017). “An empirical analysis of smart contracts: platforms, applications”. Disponible en: <https://arxiv.org/pdf/1703.06322.pdf> (fecha de consulta: 15 de mayo de 2020).

BAYLE, A., KOSCINA, M., MANSET, D., & PEREZ-KEMPNER, O. (2018). “When blockchain meets the right to be forgotten: technology versus law in the healthcare industry”, *IEEE/WIC/ACM International Conference on Web Intelligence*, pp. 788-792. Disponible en: <http://www.myhealthmydata.eu/wp->

[content/uploads/2019/10/When_Blockchain_Meets_the_Right_to_be_Forgotten.pdf](#) (fecha de consulta: 9 de junio de 2022).

BECKER, K. (2022). “Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries”, *Law and Critique*, Vol. 33, No. 2. Disponible en: <https://link.springer.com/article/10.1007/s10978-021-09317-8> (fecha de consulta: 23 de junio de 2022).

BELK, R., HUMAYUN, M., & BROUARD, M. (2022). “Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets”, *Journal of Business Research*, Vol. 153, pp.198-205. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0148296322007147> (fecha de consulta: 23 de septiembre de 2022).

BERBERICH, M., & STEINER, M. (2016). “Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers”, *European Data Protection Law Review*, Vol. 2, no. 3, pp. 422-426. Disponible en: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=71&id=&page=> (fecha de consulta: 6 de mayo de 2022)

BÉRES, F., SERES, I. A., BENCZÚR, A. A., & QUINTYNE-COLLINS, M. (2021). “Blockchain is watching you: Profiling and deanonymizing ethereum users”, *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Disponible en: <https://arxiv.org/abs/2005.14051> (fecha de consulta: 26 de marzo de 2022).

BEYER, S. (2020) “The 5 Most Common Smart Contract Vulnerabilities”. Disponible en: <https://medium.com/cryptronics/the-5-most-common-smart-contract-vulnerabilities-738de4fae3ba> (fecha de consulta: 12 de noviembre de 2020).

BIRYUKOV, A., KHOVRATOVICH, D. & PUSTOGAROV, I. (2014), “Deanonymisation of clients in Bitcoin P2P network”, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. Disponible en: <https://dl.acm.org/doi/10.1145/2660267.2660379> (fecha de consulta: 23 de enero de 2022).

BLACKBURN, A., HUBER, C., ELIAZ, Y., SHAMIM, M. S., WEISZ, D., SESHADRI, G., KIM, K., HANG, S. & AIDEN, E. L. (2022). “Cooperation among an anonymous

- group protected Bitcoin during failures of decentralization”. Disponible en: <https://arxiv.org/abs/2206.02871> (fecha de consulta: 16 de septiembre de 2022).
- BODÓ, B., GIANNOPOULOU, A., QUINTAIS, J., & MEZEI, P. (2022). “The rise of NFTs: These aren't the droids you're looking for”. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4000423 (fecha de consulta: 12 de septiembre de 2022).
- BORSELLI, A. (2020). "Smart Contracts in Insurance: A Law and Futurology Perspective", *InsurTech: A Legal and Regulatory View*, (Dirs. MARANO, P. & NOUSSIA, K.), Ed.: Springer International Publishing, pp. 101-125. Disponible en: https://doi.org/10.1007/978-3-030-27386-6_5 (fecha de consulta: 16 de agosto de 2020).
- BOUCHER, P., NASCIMENTO, S., & KRITIKOS, M. (2017). *Cómo puede cambiar nuestra vida la tecnología de la cadena de bloques*. Brussels: European Parliament. Disponible en: http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0217043ESN (fecha de consulta: 19 de septiembre de 2019).
- BOUGUERA, A. (2019). “How Will Quantum Computing Affect Blockchain?”. Disponible en: <https://consensys.net/blog/blockchain-development/how-will-quantum-supremacy-affect-blockchain/> (fecha de consulta: 1 de octubre de 2020).
- BOURQUE, S. & FUNG LING TSUI, S. (2014). “A Lawyer’s Introduction to Smart Contracts”, *Scientia Nobilitat: Reviewed Legal Studies*, Poland, pp. 4-24.
- BROWN, R.G (2018). “The corda platform: An introduction”. Disponible en: <https://www.corda.net/content/corda-platform-whitepaper.pdf> (fecha de consulta: 21 de noviembre de 2019).
- BROWN, R.G (2016). “Introducing r3 corda™: a distributed ledger designed for financial services”. Disponible en: <https://gandal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/> (fecha de consulta: 21 de noviembre de 2019).
- BRYANOV, K. (2021). “Crypto’s fraught relationship with Elon Musk: Ambassador or liability?”. Disponible en: <https://cointelegraph.com/news/crypto-s-fraught->

- [relationship-with-elon-musk-ambassador-or-liability](#) (fecha de consulta: 15 de agosto de 2022).
- BROWN, R.G., CARLYLE, J.R., GRIGG, I. & HEARN, M. (2016). “Corda: An Introduction.”. Disponible en: <https://www.corda.net/content/corda-platform-whitepaper.pdf> (fecha de consulta: 21 de noviembre de 2019).
- BUCHWALD, M. (2019). “Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration”, *University of Pennsylvania Law Review*, Vol. 168, pp. 1369-1423. Disponible en: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn-law-review> (fecha de consulta: 30 de enero de 2021).
- BUOCZ, T., EHRKE-RABEL, T., HÖDL, E., & EISENBERGER, I. (2019). “Bitcoin and the GDPR: allocating responsibility in distributed networks”, *Computer Law & Security Review*, Vol. 35, No. 2. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0267364918303170> (fecha de consulta: 2 de enero de 2022).
- LOIS-CABALLÉ, A. (2021). “Mecanismos de protección del consumidor en la propuesta de reglamento relativo a los mercados de criptoactivos”, *Guía de criptoactivos MiCA*, (Dirs. MADRID PARRA, A, PASTOR SEMPERE, M. & BLANCO SANCHEZ, M.) Ed.: Aranzadi Thomson Reuters, pp. 25-40.
- CACHERO, P. (2022). “Crypto Collapse Threatens to Leave Black, Hispanic Investors Further”. Disponible en: <https://www.bloomberg.com/news/articles/2022-07-07/crypto-collapse-threatens-to-leave-black-hispanic-investors-further-behind> (fecha de consulta: 23 de septiembre de 2022).
- CALVO CARAVACA, A. & CARRASCOSA GONZÁLEZ, J. (2020). “Contratos internacionales”, *Tratado de derecho internacional privado Tomo III*, (Dirs. CALVO CARAVACA, A. & CARRASCOSA GONZÁLEZ, J), Ed.: Tirant lo Blanch, Valencia, España, pp. 2798- 3059.
- CAMENISCH, J., DERLER, D., KRENN, S., PÖHLS, H.C., SAMELIN, K., SLAMANIG, D. (2017). “Chameleon-Hashes with Ephemeral Trapdoors” *ACR International Workshop on Public Key Cryptography*, (Dirs. FEHR, S.), Ed.: Springer, Berlin, Heidelberg. Disponible en: https://doi.org/10.1007/978-3-662-54388-7_6 (fecha de consulta: 20 de junio de 2022).

- CAMPUZANO-DIAZ, B. (2004). “El plan de acción para un Derecho contractual europeo más coherente”, *Anuario Mexicano de Derecho Internacional*, pp. 289-309. Disponible en: https://idus.us.es/bitstream/handle/11441/16281/1/file_1.pdf?sequence=1 (fecha de consulta: 23 de septiembre de 2021).
- CANAL LUNATICOIN. (2019). “Aragon Network con su Cofundador Jorge Izquierdo”. Disponible en: <https://youtu.be/m3EEVrZYa2o> (fecha de consulta: 22 de febrero de 2021).
- CANNARSA, M. (2019). “Contract Interpretation” *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dir. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 102-117.
- CASABURO, D. (2022). “Distributed Ledger Technologies and GDPR’s right to be forgotten: Can they get along?”. Disponible en: <https://www.law.kuleuven.be/citip/blog/distributed-ledger-technologies-and-gdprs-right-to-be-forgotten/> (fecha de consulta: 5 de mayo de 2022).
- CASINO, F., DASAKLIS, T.K. y PATSAKIS, C. (2019). "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, Vol. 36, pp. 55-81. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0736585318306324> (fecha de consulta: 20 de octubre de 2021).
- CASSANO, J. (2014). “What Are Smart Contracts? Cryptocurrency’s Killer App”. Disponible en: <https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app> (fecha de consulta: 16 de agosto de 2020).
- CENGIZ, F. (2021). “What the EU’s new MiCA regulation could mean for cryptocurrencies”, Disponible en: <https://blogs.lse.ac.uk/euoppblog/2021/07/05/what-the-eus-new-mica-regulation-could-mean-for-cryptocurrencies/> (fecha de consulta: 15 de agosto de 2022).
- CHAINALYSIS. (2022). “Mid-year Crypto Crime Update: Illicit Activity Falls With Rest of Market, With Some Notable Exceptions”. Disponible en: <https://blog.chainalysis.com/reports/crypto-crime-midyear-update-2022/> (fecha de consulta: 12 de septiembre de 2022).

- CHAINALYSIS. (2022). *The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime*. Disponible en: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf> (fecha de consulta: 8 de agosto de 2022).
- CHAINALYSIS. (2022). “Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity”. Disponible en: <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/> (fecha de consulta: 8 de agosto de 2022).
- CHAINALYSIS. (2021). “The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs”. Disponible en: <https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/> (fecha de consulta: 8 de agosto de 2022).
- CHAINALYSIS (2021) Who’s Who on the Blockchain? Mapping the Key Players in the Cryptocurrency Ecosystem. Disponible en: <https://go.chainalysis.com/rs/503-FAP-074/images/Key-players-in-crypto-report.pdf> (fecha de consulta: 15 de septiembre de 2022).
- CHAMBER OF DIGITAL COMMERCE. (2018). “Smart Contracts” Legal Primer Why Smart Contracts Are Valid Under Existing Law and Do Not Require Additional Authorization to Be Enforceable”. Disponible en: <https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf> (fecha de consulta: 29 de febrero de 2019).
- CHANDRASEKERA, S. (2020). “IRS Is Trying To Deanonymize Privacy Coins Like Monero And Zcash”. Disponible en: <https://www.forbes.com/sites/shehanchandrasedkera/2020/07/06/irs-is-trying-to-deanonymize-privacy-coins-like-monero-and-zcash/?sh=433ce9374174> (fecha de consulta: 10 de mayo de 2022).
- CHEN, H., PENDLETON, M., NJILLA, L., & XU, S. (2020). “A survey on ethereum systems security: Vulnerabilities, attacks, and defenses”, *ACM Computing Surveys*, Vol. 53, No. 3. Disponible en: <https://dl.acm.org/doi/fullHtml/10.1145/3391195> (fecha de consulta: 15 de noviembre de 2020).
- CHIA, V., HARTEL, P., HUM, Q., MA, S., PILIOURAS, G., REIJSBERGEN, D., VAN STAALDUINEN, M. & SZALACHOWSKI, P. (2018). “Rethinking blockchain

- security: Position paper”, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData)*, pp. 1273-1280. Disponible en: <https://ieeexplore.ieee.org/document/8726738/authors#authors> (fecha de consulta: 23 de septiembre de 2022).
- CIEPLAK, J. & LEEFATT, S. (2017). “Smart Contracts: A Smart Way to Automate Performance”, *Georgetown law technology review*, Vol. 1, pp. 414-418. Disponible en: <https://georgetownlawtechreview.org/smart-contracts-a-smart-way-to-automate-performance/GLTR-04-2017/> (fecha de consulta: 9 de abril de 2020).
- CLACK, C. (2018). “Smart Contract Templates: legal semantics and code validation”, *Journal of Digital Banking*, Vol. 2, no 4. Disponible en: https://www.researchgate.net/publication/335465751_Smart_Contract_Templates_legal_semantics_and_code_validation_C_D_Clack_Journal_of_Digital_Banking_2_4_338-352_2018. (fecha de consulta: 16 de julio de 2020).
- CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). "Smart Contract Templates: foundations, design landscape and research directions". Disponible en: <https://arxiv.org/abs/1608.00771> (fecha de consulta: 10 de mayo de 2020).
- CLACK, C., BAKSHI, V.A. & BRAINE, L. (2016). “Smart Contract Templates: essential requirements and design options”. Disponible en: <https://arxiv.org/abs/1612.04496> (fecha de consulta: 10 de mayo de 2020).
- CLACK, C., & MCGONAGLE, C. (2019). “Smart Derivatives Contracts: the ISDA Master Agreement and the automation of payments and deliveries”. Disponible en: <https://arxiv.org/abs/1904.01461> (fecha de consulta: 10 de mayo de 2020).
- CLARK, D. (1988). "The design philosophy of the DARPA internet protocols | Symposium proceedings on Communications architectures and protocols", *Computer Communication Review*, Vol. 18, No. 4, pp. 106-114. Disponible en <https://dl.acm.org/doi/abs/10.1145/52324.52336> (fecha de consulta: 1 de noviembre de 2019).
- CLAUSE. (2019). “Smart Legal Contracts on Enterprise Blockchains: A Corda Example”. Disponible en: <https://medium.com/inside-r3/smart-legal-contracts-on-enterprise->

[blockchains-an-r3-corda-example-446957b1b4ba](#) (fecha de consulta: 4 de octubre de 2020).

CLIFFORD CHANCE. (2018). *Global intellectual property newsletter Blockchain, AI and other IP topics*, Vol. 3. Disponible en: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2018/03/global-intellectual-property-newsletter-17th-issue-blockchain-ai-and-other-ip-topics.pdf> (fecha de consulta: 23 de mayo de 2022).

CLIFFORD CHANCE. (2017). "Are smart contracts contracts?". Disponible en: <https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/are-smart-contracts-contracts.html> (fecha de consulta: 9 de abril de 2020).

CODELEGIT. (Sin fecha). "CodeLegit White Paper on Blockchain Arbitration". Disponible en: https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit#heading=h.r6m6m18drsxo (fecha de consulta: 22 de marzo de 2021).

COHNEY, S., HOFFMAN, D., SKLAROFF, J. & WISHNICK, D. (2019). "Coin-Operated Capitalism", *Columbia Law Review*, Vol. 119, No. 3, pp. 591-676. Disponible en: https://scholarship.law.upenn.edu/faculty_scholarship/2027 (fecha de consulta: 27 de marzo de 2020).

COLLIER, K. (2021). "Crypto exchanges keep getting hacked, and there's little anyone can do". Disponible en: <https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870> (fecha de consulta: 21 de agosto de 2022).

CONSEJO DE LA UE Y CONSEJO EUROPEO. (2022). "Finanzas digitales". Disponible en: <https://www.consilium.europa.eu/es/policies/digital-finance/#:~:text=El%20paquete%20tiene%20por%20objeto,consumidores%20y%20la%20estabilidad%20financiera> (fecha de consulta: 16 de octubre de 2022).

COMELLES, C. (2020). "Smart contracts o Code is Law: soluciones legales para la robotización contractual *InDret: Revista para el Análisis del Derecho*, no 4. Disponible en: <https://indret.com/smart-contracts-o-code-is-law-soluciones-legales-para-la-robotizacion-contractual/> (fecha de consulta: 20 de noviembre de 2020).

- COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2017). *Notas técnicas de la CNUDMI sobre la solución de controversias en línea*, Viena. Disponible en: <https://uncitral.un.org/es/texts/online-dispute> (fecha de consulta: 15 de febrero de 2021).
- COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2013). *Solución de controversias por vía informática en las operaciones transfronterizas de comercio electrónico: visión general de los mecanismos privados de ejecución*, Viena. Disponible en: <https://undocs.org/A/CN.9/WG.III/WP.124> (fecha de consulta: 30 de enero de 2021).
- COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL. (2011). *La solución por vía informática de controversias surgidas a raíz de operaciones transfronterizas de comercio electrónico: cuestiones que deberán examinarse para elaborar un marco global que rija la solución de controversias por vía informática (ODR)*, Viena. Disponible en: https://uncitral.un.org/es/working_groups/3/online_dispute (fecha de consulta: 30 de enero de 2021).
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2020). “Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD (1.ª parte) Versión 2.0 Adoptadas el 7 de julio de 2020”. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfs_engine_after_public_consultation_es.pdf (fecha de consulta: 6 de junio de 2022).
- COMPART, C., LUINETTI, M., & PORTIER, B. (2018). “Blockchain and GDPR: How blockchain could address five areas associated with GDPR compliance”, *IBM Security White Paper*. Disponible en: <https://iapp.org/resources/article/blockchain-and-gdpr/> (fecha de consulta: 16 de mayo de 2022).
- CONTI, R. & SCHMIDT, J. (2022). “What Is An NFT? Non-Fungible Tokens Explained”. Disponible en: <https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token/> (fecha de consulta: 12 de septiembre de 2022).
- CORRALES, M, JURCYS, P. & KOUSIOURIS, G. (2019). “Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework” *Legal Tech, Smart Contracts*

- and Blockchain*, (Dir. CORRALES, M., FENWICK, M., & HAAPIO, H.), Ed.: Springer Nature, Singapur, pp. 189-220.
- CNIL. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf (fecha de consulta: 9 de octubre de 2021).
- CZARNECKI, J. (2018). "Who is the data controller in a blockchain?". Disponible en: <https://newtech.law/en/who-is-the-data-controller-in-a-blockchain/> (fecha de consulta: 7 de julio de 2022).
- DAOUI, S., FLEINERT-JENSEN, T., & LEMPERIERE, M. (2019). "GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions", *Stanford Journal of Blockchain Law & Policy*, vol 2. Disponible en: <https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france/release/1> (fecha de consulta: 2 de mayo de 2022).
- DEIBERT, R., PALFREY, J., ROHOZINSKI, R. & ZITTRAIN, J. (2007). *Access Denied the Practice and Policy of Global Internet Filtering*, MIT Press, Cambridge.
- DE FILIPPI, P. (2016). "The interplay between decentralization and privacy: the case of blockchain technologies", *Journal of Peer Production*, No.7. Disponible en: <https://hal.archives-ouvertes.fr/hal-01382006/document> (fecha de consulta: 7 de diciembre de 2021).
- DE FILIPPI, P. & HASSAN, S. (2016). "Blockchain technology as a regulatory technology: From code is law to law is code", *First Monday*, Vol. 21, No. 12. Disponible en: <https://doi.org/10.5210/fm.v21i12.7113> (fecha de consulta: 16 de marzo de 2019).
- DE FILIPPI, P. & WRIGHT, A. (2018). *Blockchain and the Law The Rule of Code*, Harvard University Press, United State Of America.
- DE LA CUESTA-RUTE. J. (2011). "Sobre la unificación del Derecho privado patrimonial en Europa", *Unificación del derecho patrimonial europeo marco común de referencia y derecho español*, (Dir. VALPUESTA GASTAMINZA, E.), Ed.: Bosch, Barcelona, pp. 23-60.
- DELL'ERBA, M. (2019). "Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public

- Regulation”, *University of Pennsylvania Journal of Law & Public Affairs*. Disponible en: <https://ssrn.com/abstract=3228445> (fecha de consulta: 2 de agosto de 2019).
- DE OLIVEIRA, F., GRIGG, I., PEREIRA, R. & CARCAZERE, L. (2017). “Triple entry ledgers with blockchain for auditing” *International Journal of Auditing Technology*, Vol. 3, no 3, p. 163-183. Disponible en: <https://doi.org/10.1504/IJAUDIT.2017.086741> (fecha de consulta: 12 de septiembre de 2020).
- DEWEY, J. (2016). “What if we developed legal contracts like we developed software applications?”. Disponible en: <https://medium.com/@ConsenSys/what-if-we-developed-legal-contracts-like-we-developed-software-applications-1b5bc8fbb915> (fecha: de consulta 21 de julio de 2020).
- DIEHL, S.T. (Sin fecha) “The Handwavy Technobabble Nothingburger” Disponible en: <https://www.stephendiehl.com/blog/nothing-burger.html> (fecha de consulta: 1 de noviembre de 2021).
- DÍEZ-PICAZO, I (2012). *Fundamentos del derecho civil patrimonial I introducción: teoría del contrato*, Thomson Civitas, Madrid.
- DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C. (2019). “Smart Contracts and Contract Law”, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 3-18.
- DIMOV, D. (2017). *Crowdsourced online dispute resolution*, Leiden University Center for Law and Digital Technologies. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003815 (fecha de consulta: 21 de marzo de 2021).
- DI PAULA, R. (2022). “¿Cómo funciona el esquema de estafas "rug pull" en el mundo de las criptomonedas?” Disponible en: <https://es.cointelegraph.com/news/how-does-the-rug-pull-work-with-cryptocurrencies> (fecha de consulta: 16 de septiembre de 2022).

- DIVER, L. (2018). "Law as a User: Design, Affordance, and the Technological Mediation of Norms", *SCRIPTed*, Vol. 15, No. 1. Disponible en: <https://script-ed.org/?p=3534> (fecha de consulta: 2 de 2020).
- DOMÍNGUEZ-GALLEGO, I. (2021). "Los elementos esenciales del contrato", *Manual de derecho civil. Vol. 2, Obligaciones y contratos, Teoría general*, (Dirs. LLAMAS-POMBO, E.), Ed.: Wolters Kluwer, Las Rozas Madrid, pp.307-327.
- DRESCHER, D. (2017). *Blockchain Basics A Non-Technical Introduction in 25 Steps*, Apress, Berkeley, California.
- DUPONT, J., & SQUICCIARINI, A. C. (2015, March). "Toward de-anonymizing bitcoin by mapping users' location", *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. Disponible en: <https://dl.acm.org/doi/10.1145/2699026.2699128> (fecha de consulta: 25 de marzo de 2022).
- DUROVIC, M. & JANSSEN, A. (2019). "Formation of Smart Contracts under Contract Law", *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 61-79.
- DUROVIC, M., & JANSSEN, A. (2019). "The Formation of Blockchain-based Smart Contracts in the Light of Contract Law", *European Review of Private Law*, pp. 753-772. Disponible en: <http://static.ie.edu.s3.amazonaws.com/Tertulia/Papers%202018/Papers/The%20Formation%20of%20Blockchain-based%20Smart%20Contracts%20in%20the.pdf> (fecha de consulta: 23 de septiembre de 2021).
- EBERHARDT, J., TAI, S. (2017). "On or Off the Blockchain? Insights on Off-Chaining Computation and Data" *European Conference on Service-Oriented and Cloud Computing*, (Dirs. DE PAOLI, F., SCHULTE, S., BROCH JOHNSEN, E.), Ed.: Springer, Cham. Disponible en: https://doi.org/10.1007/978-3-319-67262-5_1 (fecha de consulta: 9 de junio de 2022).
- ECHEBARRÍA SÁENZ, M. (2017). "Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain", *Revista de estudios europeos*, No. 70, pp. 69-97. ISSN 1132-7170. Disponible en <http://uvadoc.uva.es/handle/10324/28434> (fecha de consulta: 16 de abril de 2019).

- EENMAA-DIMITRIEVA, H. & SCHMIDT-KESSEN, M.J. (2019). "Creating markets in no-trust environments: The law and economics of smart contracts", *Computer Law & Security Review*, Vol. 35, No. 1, pp. 69-88, ISSN 0267-3649. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918303558> (fecha de consulta: 2 de abril de 2019).
- EL EMAM, K., & ALVAREZ, C. (2015). "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, Vol. 5 No. 1. Disponible en: <https://academic.oup.com/idpl/article-abstract/5/1/73/2863828?redirectedFrom=fulltext&login=true> (fecha de consulta: 3 de agosto de 2021).
- ETHEREUM. (2020). "[Spanish] White Paper Ethereum". Disponible en: <https://github.com/ethereum/wiki/wiki/%5BSpanish%5D-White-Paper.md> (fecha de consulta: 10 de junio de 2020).
- ESMA. (2019). *Advice on Initial Coins Offerings and CryptoAssets*. Disponible en https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf. (fecha de consulta: 23 de agosto de 2022).
- ESTEBAN DE LA ROSA, F. (2017). "Régimen de las reclamaciones de consumo transfronterizas en el nuevo Derecho europeo de resolución alternativa y en línea de litigios de consumo", *Revista Española de Derecho Internacional*, Vol. 69, pp. 109-137. Disponible en: http://www.revista-redi.es/wp-content/uploads/2017/07/4_estudios_esteban_de_la_rosa_regimen_reclamaciones_consumo_transfronterizas.pdf (fecha de consulta: 22 de enero de 2023).
- ESTEBAN DE LA ROSA, F. (2011). "Principios de protección del consumidor para una iniciativa europea en el ámbito de la resolución electrónica de diferencias (ODR) de consumo transfronterizas", *Revista General de Derecho Europeo*, No. 25. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2502355 (fecha de consulta: 21 de enero de 2023).
- EUROPEAN LAW INSTITUTE. (2022). *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection Council Draft*. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology_Smart_Contracts_and_Consumer_Protection_Council_Draft.pdf (fecha de consulta: 12 de agosto de 2022).

- EUROPEAN PARLIAMENT, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (2020). *Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?* Disponible en:
[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf) (fecha de consulta: 1 de junio de 2021).
- EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FÓRUM. (2018). *Blockchain And the GDPR*. Disponible:
https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (fecha de consulta: 16 de junio de 2021).
- EUROPEAN UNION, ARTICLE 29 DATA PROTECTION WORKING PARTY (2013). *Opinion 03/2013 on purpose limitation*. Disponible en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (fecha de consulta: 23 de junio de 2021).
- EUROPEAN UNION, ARTICLE 29 DATA PROTECTION WORKING PARTY (2010). *Opinion 1/2010 on the concepts of "controller" and "processor"*. Disponible en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (fecha de consulta: 25 de junio de 2022).
- EVANS, T. M. (2019). "Role of International Rules in Blockchain-Based Cross-Border Commercial Disputes", *Wayne L. Rev.*, Vol. 65, pp. 9-10. Disponible en:
https://scholars.unh.edu/cgi/viewcontent.cgi?article=1432&context=law_facpub (fecha de consulta: 16 de febrero de 2021).
- FARMER, W. & HU, Q. (2018). "FCL: A Formal Language for Writing Contracts", *Quality Software Through Reuse and Integration*, (Dirs. RUBIN, S. & BOUABANA-TEBIBEL, T.), Ed.: Springer International Publishing, pp. 190-208.
- FEIGN, A. (2022). "What Is Blockchain Technology?". Disponible en
<https://www.coindesk.com/learn/what-is-blockchain-technology/> (fecha de consulta: 2 de diciembre de 2022).
- FELIÚ, R. (2018). "Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado", *La Ley Mercantil*, No. 47.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247775 (fecha de consulta: 23 de septiembre de 2021).

- FELTEN, E. (2017). “Smart Contracts: Neither Smart nor Contracts?”. Disponible en: <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/> (fecha de consulta: 25 de junio de 2020).
- FENG, Q., HE, D., ZEADALLY, S., KHAN, M.K. & KUMAR, N. (2019). “A survey on privacy protection in blockchain system,” *Journal of Network and Computer Applications*, Vol. 126, pp. 45-58. Disponible en: <https://www.sciencedirect.com/science/article/pii/S1084804518303485#bib48> (fecha de consulta: 15 de abril de 2020).
- FERNANDEZ, L. (2018). “Diez claves para entender qué es el 'regtech'”. Disponible en: <https://tinyurl.com/y55q8vpw> (fecha de consulta: 20 de febrero de 2020).
- FERREIRA, A. & SANDNER, P. (2021). “Eu search for regulatory answers to crypto assets and their place in the financial markets’ infrastructure”, *Computer Law & Security Review*, Vol. 43. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0267364921001059> (fecha de consulta: 14 de septiembre de 2022).
- FERREIRA, A., SANDNER, P. G., & DÜNSER, T. (2021). “Cryptocurrencies, DLT and crypto assets—the road to regulatory recognition in Europe”. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891401 (fecha de consulta: 14 de septiembre de 2022).
- FINCK, M. (2017). “Blockchains and Data Protection in the European Union”, *Max Planck Institute for Innovation & Competition Research*, Paper 18-01. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (fecha de consulta: 17 de enero de 2022).
- FINCK, M., & PALLAS, F. (2020). “They who must not be identified—distinguishing personal from non-personal data under the GDPR”, *International Data Privacy Law*, Vol. 10, No. 1. Disponible en: <https://academic.oup.com/idpl/article/10/1/11/5802594> (fecha de consulta: 5 de agosto de 2022).
- FOSTER-FRAU, S. (2021) “Locked out of traditional financial industry, more people of color are turning to cryptocurrency”. Disponible en: <https://www.washingtonpost.com/national/locked-out-of-traditional-financial-industry-more-people-of-color-are-turning-to-cryptocurrency/2021/12/01/a21df3fa->

- [37fe-11ec-9bc4-86107e7b0ab1_story.html](#) (fecha de consulta: 15 de agosto de 2022).
- FREEDOM HOUSE. (2018). Freedom on the net 2018: The rise of digital authoritarianism. Disponible en https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf (fecha de consulta: 5 de enero de 2020).
- FU, J. (2020). "Algorithmic contracts: who is to blame?", *Singapore Law Review*, Vol. 12. Disponible en: <https://www.singaporelawreview.com/juris-illuminae-entries/2020/algorithmic-contracts> (fecha de consulta: 1 de diciembre de 2020).
- GALLOWAY, S. (2022). "The False Promise of Web3". Disponible en: <https://marker.medium.com/the-false-promise-of-web3-7e6c1a00d4be> (fecha de consulta: 18 de septiembre de 2022).
- GAO, Y., SHI, J., WANG, X., SHI, R., YIN, Z., & YANG, Y. (2021). "Practical Deanonimization Attack in Ethereum Based on P2P Network Analysis", *IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking*. Disponible en: <https://ieeexplore.ieee.org/document/9644904/references#references> (fecha de consulta: 26 de marzo de 2022).
- GARCÍA-VICENTE, J. (2013). "Sección segunda. del objeto de los contratos", *Comentarios al Código civil tomo VII (Arts. 1265 a 1484) (DIRS. BERCOVITZ-RODRIGUEZ-CANO, R.)*, Ed.: Tirant Lo Blanch, Valencia, pp. 9136-9140.
- GERHARDT, D. & THAW, D. (2020). "Bot contracts", *Arizona Law Review*, pp. 8787-902. Disponible en: <https://ssrn.com/abstract=3533517> (fecha de consulta: 18 de agosto de 2020).
- GIANCASPRO, M. (2017). "Is a 'smart contract' really a smart idea? Insights from a legal perspective", *Computer Law & Security Review*, Vol. 33, No. 6, pp. 825-835. ISSN 0267-3649. Disponible en: <http://www.sciencedirect.com/science/article/pii/S026736491730167X> (fecha de consulta: 16 de abril de 2019).

- GIANNOPOULOU, A. (2020). "Data Protection Compliance Challenges for Self-sovereign Identity", *Congress on Blockchain and Applications*. Disponible en: https://link.springer.com/chapter/10.1007%2F978-3-030-52535-4_10 (fecha de consulta: 23 de octubre de 2021).
- GIANNOPOULOU, A., & FERRARI, V. (2018). "Distributed data protection and liability on blockchains, *International Conference on Internet Science*. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316954 (fecha de consulta: 28 de septiembre de 2021).
- GIESSEN, D. (2019). *Blockchain and the GDPR's right to erasure*, Bachelor's thesis. Disponible en: <https://essay.utwente.nl/78738/> (fecha de consulta: 20 de junio de 2022).
- GOLDEN DATA LAW (2019) "Blockchain: Challenges and solutions for compliance with the GDPR" Disponible en: <https://medium.com/golden-data/blockchain-challenges-and-solutions-for-compliance-with-the-gdpr-c354987f8fae> (fecha de consulta: 3 de abril de 2022).
- GOLDEN DATA LAW. (2019). "Right to rectification under EU data protection law". Disponible en: <https://medium.com/golden-data/right-to-rectification-35ec099df2fc> (fecha de consulta: 20 de junio de 2022).
- GOLDEN DATA LAW. (2018). "Material scope of EU data protection law". Disponible en: <https://medium.com/golden-data/material-scope-of-eu-data-protection-law-39ecd18f7ff6> (fecha de consulta: 1 de junio de 2021).
- GOLDENFEIN, J. & LEITER, A. (2018). "Legal engineering on the blockchain: Smart contracts as legal conduct", *Law and Critique*, Vol. 29, No. 2, pp. 141-149. Disponible en: <https://link.springer.com/article/10.1007/s10978-018-9224-0> (fecha de consulta: 3 de febrero de 2021).
- GOLDSMITH, J. & WU T. (2006). *Who controls the internet? illusions of a borderless world*, Oxford University Press, Inc.
- GOVERNATORI, G., IDELBERGER, F., MILOSEVIC, Z., RIVERET, R., SARTOR, G. & XU, X. (2018). "On legal contracts, imperative and declarative smart contracts, and blockchain systems", *Artificial Intelligence and Law*, Vol. 26, No. 4, pp. 377-

409. Disponible en: <https://link.springer.com/article/10.1007/s10506-018-9223-3> (fecha de consulta: 28 de noviembre de 2020).
- GOVERNMENT OFFICE FOR SCIENCE. (2016). *Distributed ledger technology: Blackett review. Distributed ledger technology: Beyond block chain*, UK Government Chief Scientific Adviser. Disponible en: <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>. (fecha de consulta: 20 de septiembre de 2019).
- GREENSPAN, G (2017). "The blockchain immutability myth". Disponible en: <https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/> (fecha de consulta: 21 de junio de 2022).
- GRICENKO, T. (2020). *Blockchain technology: edit or not?* MSc Research Project. Disponible en: <https://norma.ncirl.ie/4562/1/tatyanagricenko.pdf> (fecha de consulta: 21 de junio de 2022).
- GRIGG, I. (2017). "Towards A Ricardian Constitution". Disponible en: <https://steemit.com/eos/@iang/towards-a-ricardian-constitution> (fecha de consulta: 26 de agosto de 2019).
- GRIGG, I. (2004). "The Ricardian contract". Disponible en https://iang.org/papers/ricardian_contract.html (fecha de consulta: 20 de agosto de 2019).
- GRIG, I. (1998-2000). "Financial Cryptography in 7 Layers". Disponible en: <https://iang.org/papers/fc7.html> (fecha de consulta: 20 de agosto de 2019).
- GRIG, I. (Sin fecha). "The Ricardian Contract". Disponible en: <https://iang.org/ricardian/> (fecha de consulta: 20 de agosto de 2019).
- GRIMMELMANN, J. (2005). "Regulation by Software", *The Yale Law Journal*, Vol. 114, pp. 1721-1758. Disponible en: <https://papers.ssrn.com/abstract=2358693> (fecha de consulta 1 de noviembre de 2019).
- GUDKOV, A. (2020). "Crowd Arbitration: Blockchain Dispute Resolution", *Legal Issues in the Digital Age*, No. 3, pp. 59-77. Disponible en: <https://ssrn.com/abstract=3755762> (fecha de consulta: 3 de febrero de 2021).

- GUPTA, M. (2018). *Blockchain For Dummies*, John Wiley & Sons, Inc., pp. 14. Disponible en: <https://www.ibm.com/downloads/cas/36KBMBOG> (fecha de consulta: 12 de octubre de 2022).
- HARARI, Y. N. (2014). *Sapiens. De animales a dioses: una breve historia de la humanidad*. Debate.
- HART, O. & MOORE, J. (1988). "Incomplete contracts and renegotiation", *Econometrica: Journal of the Econometric Society*, Vol. 56, No. 4, pp. 755-785. Disponible en: <https://www.jstor.org/stable/1912698> (fecha de consulta: 19 de septiembre de 2019).
- HARZ, D. & KNOTTENBELT, W. (2018). "Towards Safer Smart Contracts: A Survey of Languages and Verification Methods". Disponible en: <https://arxiv.org/abs/1809.09805> (fecha de consulta: 14 de junio de 2020).
- HASSAN, S. & DE FILIPPI, P. (2017). "The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code", *Field Actions Science Reports: The Journal of Field Actions*, Vol. Special Issue 17, pp. 88-90. Disponible en: <https://papers.ssrn.com/abstract=3117630> (fecha de consulta: 31 de agosto de 2019).
- HAYES, F. (2002). "The Story So Far". Disponible en: <https://www.computerworld.com/article/2576616/the-story-so-far.html> (fecha de consulta: 16 de junio de 2020).
- HAZARD, J. & HAAPIO, H. (2017). "Wise Contracts: Smart Contracts that Work for People and Machines". *Trends and communities of legal informatics. Actas del 20th international legal informatics symposium IRIS*. Disponible en: <https://ssrn.com/abstract=2925871> (fecha de consulta: 20 de abril de 2020).
- HEARN, M., & BROWN, R.G. (2019). "Corda: A distributed ledger" Disponible en: https://docs.corda.net/_static/corda-technical-whitepaper.pdf (fecha de recuperación: 21 de noviembre de 2019).
- HEAVEN, D. (2018). "Así trabajan los detectives de robos de criptomonedas en 'blockchain'", *Technology Review*. Disponible en: <https://www.technologyreview.es/s/10171/asi-trabajan-los-detectives-de-robos-de-criptomonedas-en-blockchain> (fecha de consulta 22 de abril de 2020).
- HENRY, R., HERZBERG, A., & KATE, A (2018). "Blockchain Access Privacy: Challenges and Directions", *IEEE Security & Privacy*, vol. 16, No. 4, pp. 38-45.

- Disponible en: <https://ieeexplore.ieee.org/document/8425613> (fecha de consulta: 2 de mayo de 2022).
- HERMANS, L., IANIRO, A., KOCHANSKA, U., TÖRMÄLEHTO, V. M., VAN DER KRAAIJ, A., & SIMÓN, J. M. V. (2022), “Decrypting financial stability risks in crypto-asset markets. *Financial Stability Review*”, No. 1. Disponible en: https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202205_02~1cc6b111b4.en.html (fecha de consulta: 12 de septiembre de 2022).
- HERN, A. (2014). “New York taxi details can be extracted from anonymised data, researchers say”. Disponible en: <https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn> (fecha de consulta: 5 de agosto de 2021).
- HERRERA, F. (Sin fecha). “Blockchain, anonimización y Reglamento General de Protección de Datos”. Disponible en: <https://blog.sepin.es/2019/04/blockchain-anonimizacion-rgpd/> (fecha de consulta: 23 de enero de 2022).
- HERTIG, A. (2022).” What Is Proof-of-Work?”. Disponible en: <https://www.coindesk.com/learn/2020/12/16/what-is-proof-of-work/> (fecha de consulta: 27 de noviembre de 2022).
- HILDEBRANDT, M. (2019). *Law for Computer Scientists and Other Folk*, Oxford University Press. Disponible en: <https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g> (fecha de consulta: 18 de enero de 2020).
- HILDENBRANDT, E., SAXENA, M., RODRIGUES, N., ZHU, X., DAIAN, P., GUTH, D., MOORE, B., PARK, D., ZHANG, Y., STEFANESCU, A. & ROSU, G. (2018). "KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine", *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, pp. 204-217. Disponible en: <https://ieeexplore.ieee.org/document/8429306/authors#authors> (fecha de consulta: 14 de junio de 2020).
- HOBZA, M., & VONDRÁČKOVÁ, A. (2021). “Crypto-asset services under the draft MiCA Regulation”, *Charles University in Prague Faculty of Law Research Paper* No 2021/III/4. Disponible en: <https://ssrn.com/abstract=3984355> (fecha de consulta 8 de agosto de 2022).

- HOLLANDER, L. (2019). “The Ethereum Virtual Machine — How does it work?”. Disponible en: <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e> (fecha de consulta: 25 de junio de 2020).
- HORVATH, A (2021). “Protection of consumers provided in the proposal for a regulation of markets in crypto-assets”. Disponible en: <http://pravnifakultet.rs/wp-content/uploads/2021/06/21-Agnes-Horvath.pdf> (fecha de consulta: 10 de agosto de 2022).
- HOWE, J. (2006). “The rise of crowdsourcing”, *Wired magazine*, Vol. 14, No. 6. Disponible en: <https://www.wired.com/2006/06/crowds/> (fecha de consulta: 2 de abril de 2021).
- HUGHES, E. (1993). “A Cypherpunk’s Manifesto”. Disponible en: <https://www.activism.net/cypherpunk/manifesto.html> (fecha de consulta: 1 de diciembre de 2019).
- HUMBEECK, A. V. (2019). The blockchain-GDPR paradox. Disponible en: <https://blog.codemine.be/posts/20171121-blockchain-gdpr-paradox/> (fecha de consulta: 5 de junio de 2022).
- IBÁÑEZ, L. D., O’HARA, K., & SIMPERL, E. (2018) “On blockchains and the general data protection regulation”, *EU Blockchain Forum and Observatory*, Disponible en: https://eprints.soton.ac.uk/422879/1/BLOCKchains_GDPR_4.pdf (fecha de consulta: 2 de diciembre de 2021).
- IBM. (Sin fecha). “Intercambio electrónico de datos (EDI)”. Disponible en: <https://www.ibm.com/es-es/supply-chain/edi-electronic-data-interchange> (fecha de consulta: 20 de junio de 2020).
- IBM. (Sin fecha) “What is blockchain technology?”. Disponible en: <https://www.ibm.com/topics/what-is-blockchain> (fecha de consulta: 2 de diciembre de 2022).
- INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS. (2022). *IOSCO decentralized finance report*. Disponible en: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> (fecha de consulta: 18 de septiembre de 2022).
- INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS. (2020). *Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading*

- Platforms*. Disponible en: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf> (fecha de consulta: 23 de abril de 2021).
- IRRERA, A. (2017). "Illinois watchdog first U.S. regulator to join blockchain consortium R3" Disponible en: <https://www.reuters.com/article/us-blockchain-illinois-idUSKBN16N2FN> (fecha de consulta: 12 de enero de 2020).
- ISDA & LINKLATERS. (2017). "Whitepaper Smart Contracts and Distributed Ledger – A Legal Perspective". Disponible en: <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> (fecha de consulta: 12 de marzo de 2020).
- ISDA. (2018). "ISDA Publishes Digital Iteration of the Common Domain Model". Disponible en: <https://www.isda.org/2018/06/05/isda-publishes-digital-iteration-of-the-common-domain-model/> (fecha de consulta: 17 de agosto de 2020).
- JACKSON, M. O. (2011). "A brief introduction to the basics of game theory". Disponible en: <https://ssrn.com/abstract=1968579> (fecha de consulta: 12 de abril de 2021).
- JAGATI, S. (2021). "El hackeo de Poly Network expone los fallos de DeFi, pero la comunidad acude al rescate". Disponible en: <https://es.cointelegraph.com/news/poly-network-hack-exposes-defi-flaws-but-community-comes-to-the-rescue> (fecha de consulta: 12 de septiembre de 2022).
- JAMBERT, A. (2019). "Blockchain and the GDPR: A data protection authority point of view" *Information Security Theory and Practice 12th IFIP International Conference*, (Dir. BLAZY, O., & YEUN, C), Ed.: Springer, Cham, pp. 3-6. Disponible en: https://link.springer.com/chapter/10.1007/978-3-030-20074-9_1 (fecha de consulta: 1 de junio de 2022).
- JAWAHERI, H., AL SABAH, M., BOSHMAF, Y., & ERBAD, A. (2020). "Deanonymizing Tor hidden service users through Bitcoin transactions analysis", *Computers & Security*, Vol. 89. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404818309908#bib0013> (fecha de consulta: 21 de marzo de 2022).
- JEVREMOVIC, N. (2020). "Blockchain, Smart Contracts and ADR". Disponible en: <https://papers.ssrn.com/abstract=3699422>. (fecha de consulta: 18 de enero de 2021).

- JEVREMOVIĆ, N. (2019) “2018: In Review: Blockchain Technology and Arbitration”, *Kluwer Arbitration Blog*. Disponible en: <http://arbitrationblog.kluwerarbitration.com/2019/01/27/2018-in-review-blockchain-technology-and-arbitration/> (fecha de consulta: 1 de abril de 2021).
- JIAO J., LIN SW., SUN J. (2020) “A Generalized Formal Semantic Framework for Smart Contracts”, *Lecture Notes in Computer Science*, vol 12076, pp. 75-96. Disponible en: https://doi.org/10.1007/978-3-030-45234-6_4 (fecha de consulta: 15 de diciembre de 2020).
- JIMENEZ LINARES, M. (2020). “De los contratos inteligentes (Smart Contracts) a los contratos legales inteligentes: problemática técnico-jurídica. El contrato Blockchain”, *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (Dir. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra, pp. 325-358.
- JOHNSON, D. R., POST, D. G. (1996). “Law and Borders –The Rise of Law in Cyberspace”, *Stanford Law Review*, Vol. 48, pp. 1367-1402 Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535&download=yes (fecha de consulta: 20 de diciembre de 2019).
- JONGERIUS, S. (2019). “GDPR’s Right to be Forgotten in Blockchain: it’s not black and White”. Disponible en: <https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/> (fecha de consulta: 2 de junio de 2022).
- JUR. (2019). “Whitepaper”, Vol. 2.0.2. Disponible en: <https://jur.io/wp-content/uploads/2019/05/jur-whitepaper-v.2.0.2.pdf> (fecha de consulta: 12 de febrero de 2021).
- JURIS. (2018). “Whitepaper”, Vol. 2.0. Disponible en: <https://getjuris.com/publications/#whitepaper> (fecha de consulta: 20 de marzo de 2021).
- KAAL, W.A. & CALCATERRA, C. (2018). "Crypto Transaction Dispute Resolution", *the business lawyer*, pp. 5. Disponible en: <http://dx.doi.org/10.2139/ssrn.2992962> (Fecha de consulta: 20 de agosto de 2019).
- KADIOGLU KUMTEPE, C. (2020). “A Brief Introduction to Blockchain Dispute Resolution”, *John Marshall Law Journal*, Vol. 14, No. 2, pp. 139- 157. Disponible

- en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083107 (fecha de consulta: 15 de junio de 2022).
- KAESEBERG, T. (2019). "The Code-ification of Law and Its Potential Effects", *Stanford Journal of blockchain law and policy*, Vol. 2, No. 2. Disponible en: <https://stanford-jblp.pubpub.org/pub/codeification-of-law> (fecha de consulta: 13 de septiembre de 2019).
- KAMINSKY, D. (2021). "Salt The Fries: Some Notes On Password Complexity". Disponible en: <https://dankaminsky.com/2012/01/05/salt-the-fries-some-notes-on-password-complexity/> (fecha de consulta: 10 de septiembre de 2021).
- KÄRKI, T. (2017). "Aragon Network Jurisdiction Part 1: Decentralized Court", *Aragon Blog*. Disponible en: <https://aragon.org/blog/aragon-network-jurisdiction-part-1-decentralized-court-c8ab2a675e82> (fecha de consulta: 22 de febrero de 2021).
- KOLBER, A. (2018). "Not-so-smart blockchain contracts and artificial responsibility", *Stanford Technology Law Review*, Vol. 21, p. 198-234. Disponible en: <https://law.stanford.edu/publications/not-so-smart-blockchain-contracts-and-artificial-responsibility/> (fecha de consulta: 21 de mayo de 2020).
- KOMALAVALLI, C., SAXENA, D., & LAROIYA, C. (2020). "Chapter 14 - Overview of Blockchain Technology Concepts" *Handbook of Research on Blockchain Technology* (Dirs. KRISHNAN, S., BALAS, V., JULIE, E., ROBINSON, Y., BALAJI, S. & KUMAR, S.), Ed.: Academic Press, pp. 871-903. Disponible en: <https://www.sciencedirect.com/science/article/pii/B9780128198162000149> (fecha de consulta: 17 de noviembre de 2022).
- KOOLEN, C. (2022). "Apes Gone', but What about Consumer Protection? Applying EU Consumer Law to the Transfer of NFTs. Applying EU Consumer Law to the Transfer of NFTs". Disponible en: <https://law.kuleuven.be/ccm/blog/?p=289> (fecha de consulta: 17 de septiembre de 2022).
- KOSBA, A., MILLER, A., SHI, E., WEN, Z. PAPAMANTHOU, C. (2016). "The blockchain model of cryptography and privacy-preserving smart contracts", *2016 IEEE symposium on security and privacy*, pp. 839-858. Disponible en: <https://ieeexplore.ieee.org/document/7546538> (fecha de consulta: 12 de abril de 2020).

- KOULU, R., (2016). "Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement" *SCRIPTed*, Vol. 113, No. 1., pp. 40-69. Disponible en: <https://script-ed.org/?p=2669> (fecha de consulta: 5 de septiembre de 2019).
- KREIS, F. & KAULARTZ, M. (2019). "Smart Contracts and Dispute Resolution—A Chance to Raise Efficiency?", *ASA Bulletin*, Vol. 37, no 2, pp. 336-357. Disponible en: <https://kluwerlawonline.com/journalarticle/ASA+Bulletin/37.2/ASAB2019031> (fecha de consulta: 17 de febrero de 2021).
- LANE, M. (2022). "Shutterstock Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself". Disponible en: <https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027> (fecha de consulta: 15 de septiembre de 2022).
- LASTNAME, E. (2021). "How much does it cost to deploy a smart contract on Ethereum?" Disponible en: <https://medium.com/the-capital/how-much-does-it-cost-to-deploy-a-smart-contract-on-ethereum-11bcd64da1> (fecha de consulta: 1 de noviembre de 2021).
- LEE, F. (2022). "MiCA white papers - What obligations will crypto firms have under the new European legislation?". Disponible en: <https://www.lexology.com/library/detail.aspx?g=beb201eb-21e9-48dd-ad90-071d368c3837> (fecha de consulta: 7 de agosto de 2022).
- LEE, J. & LIU, C. (2012). "Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China", *Minnesota Journal of Law, Science, and Technology*, Vol. 13, No.1. Disponible en: <https://papers.ssrn.com/abstract=2035788> (Fecha de consulta: 20 de diciembre de 2019).
- LEGERÉN-MOLINA, A. (2020). "Smart Contracts que se ejecutan en "Blockchain", *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial* (Dirs. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra, pp. 281-325.
- LEGERÉN-MOLINA A. (2019). "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de Blockchain", *Revista de Derecho Civil*, Vol. 6, No. 1, pp. 177-237. ISSN 2341-2216. Disponible en:

<https://www.nreg.es/ojs/index.php/RDC/article/view/356> (fecha de consulta: 14 de abril de 2020).

LEGERÉN-MOLINA, A. (2018). "Los contratos inteligentes en España (La disciplina de los smart contracts) /Smart contracts in Spain; the regulation of smart contracts", *Revista De Derecho Civil*, Vol. 5, No. 2, pp. 193-241, ISSN 2341-2216. Disponible en: <https://www.nreg.es/ojs/index.php/RDC/article/view/320> (fecha de consulta: 14 de abril de 2020).

LEHDONVIRTA, V. (2016). "The blockchain paradox: Why distributed ledger technologies may do little to transform the economy". Disponible en: <https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/> (fecha de consulta: 5 de enero de 2020).

LEIMEISTER, J.M. (2010). "Collective Intelligence", *Business & Information Systems Engineering*, Vol., 2, pp. 245-248. Disponible en: <https://link.springer.com/article/10.1007%2Fs12599-010-0114-8> (fecha de consulta: 8 de abril de 2021).

LEON-ROBAYO, E. (2019). *La nueva lex Mercatoria en el derecho latinoamericano de contratos*, Tirant lo Blanch - Universidad del Rosario, Bogotá, Colombia.

LESSIG, L. (2001). *El código y otras leyes del ciberespacio*, Santillana, Madrid.

LESSIG, L. (2009). *El código 2.0*, Traficantes de sueños, Madrid.

LEVY, K. (2017). "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law", *Engaging Science, Technology, and Society*, vol 3. Disponible en: <https://estsjournal.org/article/view/107> (fecha de consulta: 8 de mayo de 2020).

LEVY, P. (1994). *L'intelligence collective: Pour une anthropologie du cyberspace*, Ed.: La Decouverte, Paris. (English edition: LEVY, P. (1997) *Collective Intelligence: Mankind's Emerging World in Cyberspace*, Plenum Press, New York.

LI, S. (2020) "[IRS Hoping to Deanonymize Monero and ZCash Privacy Coins to Prevent Cybercrime](https://blockchain.news/news/irs-hoping-deanonimize-monero-zcash-privacy-coins-prevent-cybercrime)". Disponible en: <https://blockchain.news/news/irs-hoping-deanonimize-monero-zcash-privacy-coins-prevent-cybercrime> (fecha de consulta: 23 de mayo de 2022).

- LI, Z. (2021). “Standardisation of Blockchain and Distributed Ledger Technologies—A Legal Voice from the Data Protection Law Perspective”, *25th EURAS Annual Standardisation Conference—Standards for Digital Transformation: Blockchain and Innovation (The European Academy for Standardisation*. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3892298 (fecha de consulta: 10 de septiembre de 2021).
- LIANOS, I., HACKER, P., EICH, S., & DIMITROPOULOS, G. (2019). *Regulating blockchain: techno-social and legal challenges*, Oxford University Press.
- LIM, C., SAW, T. & SARGEANT, C. (2016). “Smart Contracts: Bridging the Gap Between Expectation and Reality”. Disponible en: <https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality> (fecha de consulta: 17 de abril de 2020).
- LIPSHAW, J.M. (2019). "The Persistence of “Dumb” Contracts", *Stanford Journal of Blockchain Law & Policy*, Vol. 2, No. 1. Disponible en: <https://stanford-jblp.pubpub.org/pub/persistence-dumb-contracts/release/1> (fecha de consulta: 25 de marzo de 2020).
- LIN, R. (2016). “Salt & Pepper: Spice up your hash!”. Disponible en: <https://medium.com/@berto168/salt-pepper-spice-up-your-hash-b48328caa2af> (fecha de consulta: 10 de septiembre de 2022).
- LINOY, S., STAKHANOVA, N., & RAY, S. (2021). “De-anonymizing Ethereum blockchain smart contracts through code attribution. *International Journal of Network Management*”, Vol. 31, No 1. Disponible en <https://doi.org/10.1002/nem.2130> (fecha de consulta: 26 de marzo de 2022)
- LÓPEZ BERENGUER, J. (1950). “La identificación de las personas en la relación jurídica civil”, *Anales de la Universidad de Murcia*, PP. 289-299. Disponible en: <https://tinyurl.com/ycrdful2> (fecha de consulta: 15 de mayo de 2020).
- LÓPEZ-LAPUENTE, L., NIETO, E., SAINZ, B., SEIJO, A. & TEROL, S. (2022) “Non Fungible Tokens (NFTs)”, *Blockchain: aspectos jurídicos de su utilización (Dirs. VALPUESTA, E. & HERNANDEZ, J.) Ed.: La Ley, Las Rozas, Madrid*, pp. 147-176.

- LOPEZ-RODRIGUEZ, A. (2021).” Applicable Law to Smart Contracts and Lex Cryptographia”, *Cuadernos Derecho Transnacional*, Vol. 13, No. 1. Disponible en: <https://e-revistas.uc3m.es/index.php/CDT/article/view/5966> (fecha de consulta: 2 de diciembre de 2022).
- LOW, K. & MIK, E. (2019). "Pause the Blockchain Legal Revolution", *International & Comparative Law Quarterly*, Vol. 69, No. 1, pp. 135-175. Disponible en: <https://doi.org/10.1017/S0020589319000502> (fecha de consulta: 3 de enero de 2020).
- LOW, K. & MIK, E. (2020). “Lost in Transmission: Unilateral Mistakes in Automated Contracts”, *Law Quarterly Review*. Disponible en: <https://ssrn.com/abstract=3591657> (fecha de consulta: 1 de diciembre de 2020).
- LUMET, S. (1957). “Doce hombres sin piedad”, *Metro-Goldwyn-Mayer*. Disponible en: <https://www.filmaffinity.com/es/film695552.html> (fecha de consulta: 23 de marzo de 2021).
- MAGNUSON, W. (2020). *Blockchain democracy: Technology, law and the rule of the crowd*, Cambridge University Press.
- MAKAROV, I., & SCHOAR, A. (2022). “Blockchain analysis of the bitcoin market”. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3942181 (fecha de consulta: 26 de marzo de 2022).
- MALDONADO, J. (2020). “¿Qué es la Ethereum Virtual Machine (EVM)? La máquina virtual de Ethereum”. Disponible en: <https://es.cointelegraph.com/explained/what-is-the-ethereum-virtual-machine-evm-the-ethereum-virtual-machine> (fecha de consulta: 16 de junio de 2020).
- MALONE, T & BERNSTEIN, M. (2015). “Introduction” *Handbook of Collective Intelligence*, (Dir. MALONE, T. & BERNSTEIN, M.), MIT Press, Cambridge.
- MANTEGHI, M. (2021). “Blockchain and the European Union’s General Data Protection Regulation: from Conflict to “Peaceful” Coexistence?”. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805647 (fecha de consulta: 16 de agosto de 2021).

- MARIN-LOPEZ, M. (2020). “Requisitos esenciales del contrato. Elementos accidentales del contrato”, *Tratado de Contratos*, (Dir. BERCOVITZ, R., MORALEJO N. & QUICIOS), Ed.: Tirant lo Blanch, pp. 597-746.
- MARKETS AND MARKETS. (2021). *Crypto Asset Management Market by Solution (Custodian and Wallets), Application Type (Web-based and Mobile-based), End User (Individuals and Enterprises (Institutions (BFSI, Hedge Funds), Retail and eCommerce)), and Region - Global Forecast to 2026*. Disponible en: <https://www.marketsandmarkets.com/requestsampleNew.asp?id=201925303> (fecha de consulta: 1 de julio de 2022).
- MARKUS. (2017). “How Smart Contract arbitration works”. Disponible en: <https://codelegit.com/author/markus/> (fecha de consulta: 23 de marzo de 2021).
- MARTIN-BARITEAU, F. (2018). “Blockchain and the european union general data protection regulation: The CNIL's perspective”, *Blckchn. ca Working Paper Series*, 1. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275783 (Fecha de consulta: 2 de mayo de 2022).
- MARTÍNEZ, L. M. G. (2021). “Infraestructuras de mercado basadas en tecnología de registro distribuido (TRD): el futuro Régimen Piloto de la UE”, *Revista de derecho del mercado de valores*, No. 29. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=8263989> (fecha de consulta: 28 de septiembre de 2022).
- MARX, L. (2018). “Storing Data on the Blockchain: The Developers Guide”. Disponible en: <https://malcoded.com/posts/storing-data-blockchain/> (fecha de consulta: 5 de junio de 2022).
- MATSSON, D. (2022). *GDPR, Blockchain & Personal data-The rights of the individual v. the integrity of Blockchain*. Disponible en: https://gupea.ub.gu.se/bitstream/handle/2077/70713/gupea_2077_70713_1.pdf;jsessionid=71E241E80D447BE6170AFAAF6CD2E8C7?sequence=1 (fecha de consulta: 9 de junio de 2022).
- MATTEREUM. (2020). “Working Paper”. Disponible en: <https://mattereum.com/2020/02/03/working-paper/> (fecha de consulta: 1 de abril de 2021).

- MAY, T. (1994). “Manifiesto criptoanarquista”. Disponible en: <https://www.mises.org.es/2017/02/manifiesto-criptoanarquista/> (fecha de consulta: 20 de noviembre de 2019).
- MCJOHN, S. & MCJOHN, I. (2016). “The Commercial Law of Bitcoin and Blockchain Transactions”, *Uniform Commercial Code Law Journal*, Vol. 47, No. 2. pp. 187-222.
- MEIJER, C. R. (2018). "Blockchain versus GDPR and who should adjust most". Disponible en: <https://www.finextra.com/blogposting/16102/blockchain-> (fecha de consulta: 1 de abril de 2022).
- MESHEL, T., & YAHYA, M. A. (2021). “Crypto Dispute Resolution: An Empirical Study”, *Journal of Law, Technology and Policy*, Vol. 2021, No. 2, pp. 187-256. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3975500 (fecha de consulta: 15 de diciembre de 2021).
- METZGER, J. (2019). “The current landscape of blockchain-based, crowdsourced arbitration”, *Macquarie LJ*, Vol. 19, pp. 81-101. Disponible en: https://www.mq.edu.au/_data/assets/pdf_file/0010/866287/Blockchain-Based-Crowdsourced-Arbitration.pdf (fecha de consulta: 12 de diciembre de 2020).
- MIK, E. (2019). “Smart Contracts: A Requiem”, *Journal of Contract Law*. Disponible en: <https://ssrn.com/abstract=3499998> (fecha de consulta: 4 de mayo de 2020).
- MIK, E. (2017). “Smart contracts: Terminology, technical limitations and real world complexity”, *Law, Innovation and Technology*, vol 9, No. 2. Disponible en: https://ink.library.smu.edu.sg/sol_research/2341/ (fecha de consulta: 30 de mayo de 2020).
- MILLARD, C. (2018). "Blockchain and law: Incompatible codes?", *Computer Law & Security Review*, Vol. 34, No. 4, pp. 843-846. ISSN 0267-3649. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918302437> (fecha de consulta: 26 de abril de 2019).
- MIRCHANDANI, A. (2019). “The GDPR-blockchain paradox: exempting permissioned Blockchains from the GDPR”, *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 29, No. 4, pp.1201-1241. Disponible en:

- <https://ir.lawnet.fordham.edu/iplj/vol29/iss4/5/> (fecha de consulta: 2. De mayo de 2022).
- MITCHELL, W. (1995). *City of Bits: Space, Place, and the Infobahn*, Cambridge Massachusetts, MIT Press.
- MOEREL, L. (2019). “Blockchain and Data Protection” *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 213-232.
- MONSALVE, S. (2003). “John Nash y la teoría de juegos” *Lecturas matemáticas*, Vol. 24, no 2, pp. 137-149. Disponible en: https://www.cienciared.com.ar/ra/usr/4/26/john_nash_y_la_teor_a_de_juegos.pdf (fecha de consulta: 12 de abril de 2021).
- MONTERO-PUYOL, F. (2016). “Los principios del derecho a la protección de datos”, *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, (Dirs. PIÑAR-MAÑAS, J.), Ed.: Reus, pp. 135-150.
- MONTESINOS, A. (2021). “Inteligencia Artificial y ODR”, *Justicia algorítmica y neuroderecho*, (Dirs. BARONA-VILAR, S.), Ed: Tirant lo Blanch, pp. 507-531.
- MORALES, J.& CHOLVI, F. (2022). “Criptoactivos y sector financiero: revolución en el mercado y retos regulatorios”. Disponible en: https://www.garrigues.com/es_ES/garrigues-digital/criptoactivos-sector-financiero-revolucion-mercado-retos-regulatorios (fecha de consulta: 24 de enero de 2023).
- MORENO, M. (1999). *Contratos electrónicos*, Marcial Pons, Madrid.
- MOWSHOWITZ, A. (1984). “Computers and the myth of neutrality”. Disponible en: <http://dx.doi.org/10.1145/800014.808144> (fecha de consulta: 2 enero de 2020).
- MEYER, D. (2018). “Blockchain technology is on a collision course with EU privacy law”, *The Privacy Advisor*. Disponible en: <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/> (fecha de consulta 15 de abril de 2022).
- MYERSON, R (1997). *Game theory*, Harvard university press.

- NAKAMOTO, S. (2008). "Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer". Disponible en: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf (fecha de consulta: 2 de abril de 2019).
- NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A., & GOLDFEDER, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, Princeton University Press.
- NARAYANAN, A., SHMATIKOV, V. (2010). "Myths and fallacies of" personally identifiable information". *Communications of the ACM*, Vol. 53, No. 6, pp. 24 - 26. Disponible en: https://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf (fecha de consulta: 16 de junio de 2021).
- NARAYANAN, A., & SHMATIKOV, V. (2008,). "Robust de-anonymization of large sparse datasets", 2008 *IEEE Symposium on Security and Privacy*, pp. 111-125. Disponible en: <https://ieeexplore.ieee.org/abstract/document/4531148> (fecha de consulta: 16 de junio de 2021).
- NARAYANAN, A., & SHMATIKOV, V. (2006). "How to break anonymity of the netflix prize dataset", *arXiv preprint*. Disponible en: <https://arxiv.org/abs/cs/0610105> (fecha de consulta: 16 de junio de 2021).
- NAVA- GONZÁLEZ, W. & GONZÁLEZ-MARTÍN, N. (2022). "Panorama actual de los criptotribunales arbitrales: obstáculos y consideraciones jurídicas", *Anales de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata*, No. 52. pp. 595-608. Disponible en: <https://revistas.unlp.edu.ar/RevistaAnalesJursoc/article/view/13518> (fecha de consulta: 16 de enero de 2023)
- NEUBURGER, J. (2018). "Blockchain, Personal Data and the GDPR Right to be Forgotten". Disponible en: <https://perma.cc/2XNH-T2GA> (fecha de consulta: 1 de abril de 2022).
- NEWS EUROPEAN PARLIAMENT. (2022). "Cryptocurrency dangers and the benefits of EU legislation". Disponible en: <https://www.europarl.europa.eu/news/en/headlines/economy/20220324STO26154/cryptocurrency-dangers-and-the-benefits-of-eu-legislation> (fecha de consulta: 13 de octubre de 2022).

- NIKOLIĆ, I., KOLLURI, A., SERGEY, LL., SAXENA, P. & HOBOR, A. (2018). "Finding the greedy, prodigal, and suicidal contracts at scale", *Proceedings of the 34th Annual Computer Security Applications Conference*, PP. 653-663. Disponible en: <https://doi.org/10.1145/3274694.3274743> (fecha de consulta: 12 de noviembre de 2020).
- NORTON ROSE FULBRIGHT (2019). "Blockchain dispute risks for banks". Disponible en: <https://www.nortonrosefulbright.com/es-es/knowledge/publications/3fb55e09/blockchain-dispute-risks-for-banks> (fecha de consulta: 20 de febrero de 2021).
- NORTON ROSE FULBRIGHT. (2019). "Singapore court's cryptocurrency decision: Implications for cryptocurrency trading, smart contracts and AI". Disponible en: <https://www.nortonrosefulbright.com/en-nl/knowledge/publications/6a118f69/singapore-courts-cryptocurrency-decision-implications-for-trading-smart-contracts-and-ai> (fecha de consulta: 1 de diciembre de 2020).
- OMOHUNDRO, S. (2014). "Cryptocurrencies, smart contracts, and artificial intelligence", *AI matters*, Vol. 1, No. 2, pp. 19-21. Disponible en: <https://doi.org/10.1145/2685328.2685334> (fecha de consulta: 16 de agosto de 2020).
- OPENLAW. (2018). "OpenCourt: Legally Enforceable Blockchain-Based Arbitration". Disponible en: <https://media.consensys.net/opencourt-legally-enforceable-blockchain-based-arbitration-3d7147dbb56f> (fecha de consulta: 1 de abril de 2021).
- ORCUTT, M. (2019). "Once hailed as unhackable, blockchains are now getting hacked", *MIT Technology Review*, Disponible en: <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> (fecha de consulta: 19 de noviembre de 2020).
- ORCUTT, M. (2019). "Cómo asegurar la información que gobierna los contratos inteligentes", *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/10757/como-asegurar-la-informacion-que-gobierna-los-contratos-inteligentes> (fecha de consulta: 19 de noviembre de 2020).

- ORCUTT, M. (2018). "Ojo, los contratos inteligentes de Ethereum están llenos de fallos", *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/10049/ojo-los-contratos-inteligentes-de-ethereum-estan-llenos-de-fallos> (fecha de consulta: 2 de agosto de 2019).
- ORTOLANI, P. (2016). "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin", *Oxford Journal of Legal Studies*, Vol. 36, No. 3, pp. 595-629. Disponible en: <https://academic.oup.com/ojls/article/36/3/595/1752378> (fecha de consulta: 10 noviembre 2020).
- ORTOLANI, P. (2019). "The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads", *Uniform Law Review*, Vol. 24, No. 2, pp. 430-448. Disponible en: <https://doi.org/10.1093/ulr/unz017> (fecha de consulta: 14 de marzo de 2020).
- O'SHIELDS, R. (2017). "Smart Contracts: Legal Agreements for the Blockchain", *North Carolina Banking Institute*, Vol. 21, No. 1, pp. 177-194. Disponible en: <https://scholarship.law.unc.edu/ncbi/vol21/iss1/11/> (fecha de consulta: 1 de diciembre de 2019).
- OTERO, L. (2019). "Análisis jurídico de los smart contract". Disponible en: https://www.legaltoday.com/legaltech/novedades-legaltech/analisis-juridico-de-los-smart-contract-2019-05-23/#_ftn2 (fecha de consulta: 15 de mayo de 2020).
- PADILLA SÁNCHEZ, J. (2020). "Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos" *Revista de Derecho privado*, No. 39. Disponible en: <http://dx.doi.org/10.18601/01234366.n39.08> (fecha de consulta: 15 de noviembre de 2020).
- PAECH, P. (2016). "The Governance of Blockchain Financial Networks", *LSE Law, Society and Economy*, Documento de trabajo, no 16. Disponible en: <https://ssrn.com/abstract=2875487> (fecha de consulta: 9 de agosto de 2020).
- PAGALLO, U., BASSI, E., CREPALDI, M., & DURANTE, M. (2018). "Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure", *JURIX*, pp. 81-90. Disponible en: <https://ebooks.iospress.nl/volumearticle/50837> (fecha de consulta: 20 de mayo de 2022).

- PARDOLESI, R. & DAVOLA, A. (2019). "What is wrong in the debate about smart contracts working paper". Disponible en: <https://ssrn.com/abstract=3339421> (fecha de consulta: 16 de agosto de 2020).
- PARIZI, M., AMRITRAJ & DEHGANTANHA, A. (2018) "Smart Contract Programming Languages on Blockchains: An Empirical Evaluation of Usability and Security", *Computer Science*, Vol. 10974. pp. 75-91. Disponible en: https://doi.org/10.1007/978-3-319-94478-4_6 fecha de consulta: 25 de septiembre de 2021).
- PARK, J., LEE, D. & IN, H. (2017) "Saving deployment costs of smart contracts by eliminating gas-wasteful patterns", *International Journal of Grid and Distributed Computing*, Vol. 10, no 12, p. 53-64. Disponible en: <http://dx.doi.org/10.14257/ijgdc.2017.10.12.06> (fecha de consulta: 16 de junio de 2020).
- PASTOR, J. (2018). "Coincheck sufre el mayor robo de criptodivisas de la historia, 535 millones de dólares en NEM". Disponible en: <https://www.xataka.com/criptomonedas/coincheck-detiene-operaciones-de-retirada-de-criptodivisas-y-los-usuarios-estan-empezando-a-temer-lo-peor> (fecha de consulta: 17 de septiembre de 2022).
- PASTOR-SEMPERE, C. (2020). "La reconstrucción económica europea y el futuro Reglamento MiCA". Disponible en: <https://www.legaltoday.com/opinion/articulos-de-opinion/la-reconstruccion-economica-europea-y-el-futuro-reglamento-mica-2020-11-19/> (fecha de consulta: 24 de enero de 2023).
- PEREIRA, J. (2019). "The genesis of the revolution in Contract Law", *ACM*, pp. 374-377, ISBN 9781450366441. Disponible en: <http://dl.acm.org/citation.cfm?id=3326414>. (fecha de consulta: 25 de septiembre de 2020).
- PÉREZ CÁZARES, M. E. (2018). "La lex mercatoria una ley procesal global", *Derecho global. Estudios sobre derecho y justicia*, Vol., 3, No. 9. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362018000200104 (fecha de consulta: 2 de diciembre de 2022).
- PEREZ, H. (2022). "Servicio de criptompréstamos Celsius pausa los retiros citando "condiciones extremas del mercado". Disponible en: <https://www.diariobitcoin.com/criptomonedas/servicio-criptoprestamos-celsius->

[pausa-retiros-cita-condiciones-extremas-mercado/](#) (fecha de consulta: 15 de agosto de 2022).

PETERS, G.W. & PANAYI, E. (2016). “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money”, *Banking Beyond Banks and Money A Guide to Banking Services in the Twenty-First Century*, (Dirs. TASCA, P., TOMASO, A., PELIZZON, L. & PERONY, N.), Ed.: Springer, Cham., pp. 239-278.

POELMAN, M., & IQBAL, S. (2021). “Investigating the compliance of the GDPR: Processing personal data on a blockchain”, *IEEE 5th International Conference on Cryptography, Security and Privacy*. Disponible en <https://ieeexplore.ieee.org/abstract/document/9357590> (fecha de consulta: 14 de septiembre de 2022).

POLITOU, E., ALEPIS, E., VIRVOU, M., PATSAKIS, C. (2022). “Privacy in Blockchain” *Privacy and Data Protection Challenges in the Distributed Era. Learning and Analytics in Intelligent Systems*, (Dirs. POLITOU, E., ALEPIS, E., VIRVOU, M., PATSAKIS, C.), Ed.: Springer, Cham. 133–149. Disponible en: https://doi.org/10.1007/978-3-030-85443-0_7 (fecha de consulta: 26 de mayo de 2022).

PONCIBÒ, C. & DIMATTEO, L. (2019). “Smart Contracts Contractual and Noncontractual Remedies” *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 118-140.

POSNER, R. (2004). “The Law and Economics of Contract Interpretation”, *Texas law Review*, vol 83, pp. 1581-1614. Disponible en: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2893&context=journal_articles (fecha de consulta: 19 de septiembre de 2019).

PRICE WATERHOUSE COOPERS. (2021). *El impacto regulatorio de la Propuesta MiCA*. Disponible en: <https://www.pwc.es/es/auditoria/assets/impacto-regulatorio-mica-en%20los-criptoactivos.pdf> (fecha de consulta: 18 de agosto de 2022).

PRISCO, G. (2016). “The DAO Raises More Than \$117 Million in World’s Largest Crowdfunding to Date” Disponible en: <https://bitcoinmagazine.com/business/the->

dao-raises-more-than-million-in-world-s-largest-crowdfunding-to-date-1463422191 (fecha de consulta: 19 de diciembre de 2019).

PUERTO, M. (2007). "La regulación de Internet y la teoría jurídica", *Anuario de filosofía del derecho*, No. 24, pp. 441-464. Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=2769990> (fecha de consulta: 5 de enero de 2020).

PURTOVA, N. (2018). "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10, No. 1. Disponible: <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> (fecha de consulta: 16 de junio de 2021).

QUAMARA, S., & SINGH, A. K. (2022). "A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives". *Computers & Security*, Vol. 113. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0167404821003722> (fecha de consulta: 10 de septiembre de 2022).

QUINTENZ, B. (2018). "Remarks of Commissioner", *38th Annual GITEX Technology Week Conference*. Disponible en: <https://cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16> (fecha de consulta: 18 de septiembre de 2020).

QUIROZ-RUIZ, A. (2020). "Cuestiones jurídicas del comercio electrónico en Blockchain", *Blockchain: Impacto en los sistemas financiero, notarial, registral y judicial*, (Dirs. RUIZ-DE VALDIVIA, I), Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra, pp. 871-903.

QURESHI, H. (2017). "A hacker stole \$31M of Ether — how it happened, and what it means for Ethereum". Disponible en: <https://www.freecodecamp.org/news/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce/> (fecha de consulta: 12 de octubre de 2020).

RABINOVICH-EINY, O. & KATSH, E. (2019). "Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution". pp. 47-75. Disponible en: <https://papers.ssrn.com/abstract=3508461> (fecha de consulta: 24 de febrero de 2020).

- RAMPONE, F. (2018). "Data Protection in the Blockchain Environment: GDPR is not a Hurdle to Permissionless DLT Solutions", *Cyberspazio e diritto*, 2018, Vol. 19, No. 61, pp.3. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383619 (fecha de consulta: 20 de agosto de 2021).
- RASKIN, M. (2017). "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review*, Vol. 304, pp. 305-344. Disponible en: <http://dx.doi.org/10.2139/ssrn.2842258> (fecha de consulta: 2 de febrero de 2020).
- READ, I. I., & PEHLIVAN, C. N. (2020). "Blockchain and Data Protection: A Compatible Couple?", *Global Privacy Law Review*, Vol. 1. No. 1, pp. 39-48 Disponible en: https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/1.1/GPLR2020005_05 (fecha de consulta: 8 de junio de 2022).
- REIDENBERG, J. (1996). "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, No. 76. pp.553-593. Disponible en: https://ir.lawnet.fordham.edu/faculty_scholarship/42 (fecha de consulta 1 de noviembre de 2019).
- REZAEIGHALEH, H., & ZOU, C. C. (2019). "Deterministic sub-wallet for cryptocurrencies", *2019 IEEE International Conference on Blockchain*. Disponible en: <https://ieeexplore.ieee.org/abstract/document/8946154/references#references> (fecha de consulta: 28 de agosto de 2022).
- ROCHER, L., HENDRICKX, J. M., & DE MONTJOYE, Y. A (2019). "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, Vol. 10, No. 1. Disponible en: <https://www.nature.com/articles/s41467-019-10933-3> (fecha de consulta: 22 de agosto de 2021).
- RODRIGUES, U. (2019). "Law and the Blockchain", *Iowa Law Review*, Vol. 104, No. 2, pp. 679-729. SSN 0021-0552. Disponible en: <https://ilr.law.uiowa.edu/print/volume-104-issue-2/law-and-the-blockchain/> (fecha de consulta: 16 de abril de 2019).
- ROJAS, J. (2022). "Justicia descentralizada ¿nueva tendencia?". Disponible en: https://www.google.com/search?q=JUSTICIA+DESCENTRALIZADA+NUEVA+TENDENCIA&rlz=1C5CHFA_enES903ES903&oq=JUSTICIA+DESCENTRALI

ZADA+NUEVA+TENDENCIA&aqs=chrome..69i57j69i60.9664j0j7&sourceid=chrome&ie=UTF-8 (fecha de consulta: 18 de enero de 2023).

ROSS, D. (2019). "Game Theory", *The Stanford Encyclopedia of Philosophy*. Disponible en: <https://plato.stanford.edu/archives/win2019/entries/game-theory/> (fecha de consulta: 3 de marzo de 2021).

ROSENTHAL, D. (2022). "Regulating "Digital Assets". Disponible en: <https://blog.dshr.org/2022/07/regulating-digital-assets.html> (fecha de consulta: 1 de septiembre de 2022).

ROSENTHAL, D. (2021). "NFTs and Web Archiving". Disponible en: <https://blog.dshr.org/2021/04/nfts-and-web-archiving.html> (fecha de consulta: 7 de junio de 2022).

RÜHL, G. (2020). "Smart (Legal) "Contracts, or: Which (Contract) Law for Smart Contracts?", *Blockchain, Law and Governance*, (Dirs. CAPPIELLO B. & CARULLO G.) Ed.: Springer International Publishing, Cham, pp. 159-180.

RUSHKOFF, D. (2022). "What? Your Assets at Coinbase are Not Safe?". Disponible en: <https://rushkoff.medium.com/what-your-assets-at-coinbase-are-not-safe-3ad20708a888> (fecha de consulta: 12 de septiembre de 2022).

R3 (2017). "Other Concepts - Legal Prose" Disponible en: <https://vimeo.com/213879293> (fecha de consulta 12 de enero de 2020).

R3. (2017). "What is a Ricardian contract". Disponible en: <https://www.r3.com/blog/what-is-a-ricardian-contract/> (fecha de consulta: 28 de agosto de 2020).

SAI, A. R., BUCKLEY, J., FITZGERALD, B., & LE GEAR, A. (2021). "Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*", Vol. 58, No. 4. Disponible en: <https://www.sciencedirect.com/science/article/pii/S0306457321000844#b37> (fecha de consulta: 12 de septiembre de 2022).

SABRINA, A. (2022). "Blockchain: La tecnología de cadena de bloques". Disponible en: <https://criptoescultura.com/tecnologia-cadena-de-bloques/> (fecha de consulta: 2 de diciembre de 2022).

SÁNCHEZ RUIZ DE VALDIVIA, I. (2020). "Blockchain e inteligencia artificial: dos tecnologías que convergen e impactan en la economía y el derecho", *Blockchain:*

- impacto en los sistemas financiero, notarial, registral y judicial*, (Dirs. SANCHEZ RUIZ DE VALDIVIA, I.). Ed.: Thomson Reuters Aranzadi, S.A. Cizur Menor, Navarra. pp. 58 – 175.
- SÁNCHEZ RUIZ DE VALDIVIA, I. (2019). “Blockchain y plataformas de financiación participativa: dos retos del mercado único digital”, *Relaciones contractuales en la economía colaborativa y en la sociedad digital*, (Dirs. GARCÍA GONZÁLEZ, G., & REDINHA, M.^a R.), Ed: Dykinson, pp. 353-373.
- SÁNCHEZ RUIZ DE VALDIVIA, I. (2019). “La protección de los usuarios en los servicios prestados por las Plataformas de Financiación Participativa de préstamo”, *Propuestas de regulación de las Plataformas de Economía Colaborativa: perspectivas generales y sectoriales*, (Dirs. ORTÍ- VALLEJO, A. & RUBIO-GIMENO, G), Ed: Thomson-Reuters Aranzadi. Cizur Menor, pp. 231-256.
- SÁNCHEZ RUIZ DE VALDIVIA, I. (2018). “Plataformas de financiación participativa: una alternativa sugerente a la financiación de Pymes que facilita, también, la contratación inmobiliaria e hipotecaria transfronteriza”, *Contratación Inmobiliaria e hipotecaria transfronteriza (Análisis económico, financiero, notarial, registral, judicial, fiscal y penal)*, (Dir. SANCHEZ RUIZ DE VALDIVIA), Ed: Thomson Reuters Aranzadi, Cizur Menor, pp. 25-105.
- SANTOS-MORÓN, M. J. (2020). “Tratamiento de datos, sujetos implicados, responsabilidad proactiva”, *Protección de datos personales*, (Dirs. GONZÁLEZ-PACANOWSKA, I. & CASTILLA-BAREA, M.), Ed.: Tirant lo Blanch, pp. 23-77.
- SAYEED, S., MARCO-GISBERT, H. & CAIRA, T. (2020). “Smart Contract: Attacks and Protections”. *Ieee Access*, Vol. 8, Disponible en: <https://ieeexplore.ieee.org/document/8976179> (fecha de consulta: 15 de diciembre de 2020).
- SHAH, P., FORESTER, D., BERBERICH, M., RASPÉ, C., & MUELLER, H. (2019). “Blockchain technology: Data privacy issues and potential mitigation strategies”. *Practical Law*, pp. 6. Disponible en: [https://www.davispolk.com/sites/default/files/blockchain technology data privacy issues and potential mitigation strategies w-021-8235.pdf](https://www.davispolk.com/sites/default/files/blockchain%20technology%20data%20privacy%20issues%20and%20potential%20mitigation%20strategies%20w-021-8235.pdf) (fecha de consulta: 26 de mayo de 2022).

- SHELLEKENS, M. (2020). "Conceptualizations of the controller in permissionless blockchains", *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 11. Disponible en: <https://www.jipitec.eu/issues/jipitec-11-2-2020/5099> (fecha de consulta: 1 de julio de 2022).
- SHELLING, T. (1964). *La estrategia del conflicto*, Tecnos, Madrid.
- SHEARMAN-STERLING, LLP, R3 & BAFT. (2018). "Code Is Not Law: The Legal Background for Trade Finance Using Blockchain". Disponible en: <https://r3.com/reports/code-is-not-law-the-legal-background-for-trade-finance-using-blockchain/> (fecha de consulta: 17 de noviembre de 2019).
- SCHLEGEL, M., ZAVOLOKINA, L., & SCHWABE, G. (2018). "Blockchain technologies from the consumers' perspective: What is there and why should who care?". *Proceedings of the 51st Hawaii international conference on system sciences*, pp. 3477-3486. Disponible en: <https://www.blockchain.uzh.ch/wp-content/uploads/paper0442-1.pdf> (fecha de consulta: 10 de septiembre de 2022).
- SCHMITZ, A.J. (2020). "Resolving a New Kind of Trade War Through ODR". Disponible en: <https://papers.ssrn.com/abstract=3525767> (fecha de consulta: 24 de febrero de 2020).
- SCHMITZ, A.J. & RULE, C. (2019). "Online Dispute Resolution for Smart Contracts", *Legal Studies Research Paper Series*, Documento de trabajo No. 2019-11, pp. 103-125. Disponible en: <https://papers.ssrn.com/abstract=3410450> (Fecha de consulta: 5 de septiembre de 2019).
- SCHNEIER, B. (2007). "Why 'Anonymous' Data Sometimes Isn't". Disponible en: <https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/> (fecha de consulta: 18 de junio de 2021).
- SCHULTZ, T. (2002). *Online Dispute Resolution: an overview and selected issues*, United Nations Economic Commission for Europe, (UNECE) Forum on Online Dispute Resolution, Genova. Disponible en: <https://ssrn.com/abstract=898821> (fecha de consulta: 3 de febrero de 2021).
- (2002). "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," *Proceedings First International Conference on Peer-to-Peer Computing*, pp. 101- 102 Disponible en:

- <https://ieeexplore.ieee.org/document/990434> (fecha de consulta: 10 de mayo de 2022).
- SHUMBA, C. (2021). “BitMart suspende la retirada de dinero tras sufrir un ciberataque: los delincuentes roban 173 millones en criptomonedas con una clave privada”. Disponible en: <https://www.businessinsider.es/bitmart-sufre-ciberataque-sustraen-173-millones-criptomonedas-976183> (fecha de consulta: 12 de septiembre de 2022).
- SCHUSTER, E. (2019). “Cloud Crypto Land”, *LSE Law, Society and Economy*, documento de trabajo No. 17. Disponible en: <https://ssrn.com/abstract=3476678> (fecha de consulta: 17 de junio de 2020).
- SERGEENKOV, A. (2020). “How Ethereum Works”. Disponible en: <https://www.coindesk.com/learn/ethereum-101/how-ethereum-works> (fecha de consulta: 13 de julio de 2020).
- SHEHATA, I. (2019). “Smart Contracts & International Arbitration”. Disponible en: <https://ssrn.com/abstract=3290026> (fecha de consulta: 21 de febrero de 2021).
- SIEGEL, D. (2019). “Understanding The DAO Attack” Disponible en: <https://www.coindesk.com/understanding-dao-hack-journalists> (fecha de consulta: 19 de diciembre de 2019).
- SIMÕES, C. (2022). “¿Qué son los bloques en la tecnología Blockchain?”. Disponible en: <https://www.itdo.com/blog/que-son-los-bloques-en-la-tecnologia-blockchain/> (fecha de consulta: 27 de noviembre de 2022).
- SIMONITE, T. (2015). "Los contratos inteligentes con Bitcoin permitirán distintos tipos de crímenes", *MIT Technology Review*. Disponible en: <https://www.technologyreview.es/s/5078/los-contratos-inteligentes-con-bitcoin-permitiran-distintos-tipos-de-crmenes> (fecha de consulta: 26 de marzo de 2019).
- SIMONITE, T. (2013). “Las identidades de los usuarios de Bitcoin podrían salir al descubierto”, *Technology Review*. Disponible en: <https://www.technologyreview.es/s/3757/las-identidades-de-los-usuarios-de-bitcoin-podrian-salir-al-descubierto>. (fecha de consulta: 22 de abril de 2020).
- SINGH, J. (2021). “Private, public and consortium”. Disponible en: <https://cointelegraph.com/explained/private-public-and-consortium-blockchains->

[the-differences-explained?_ga=2.78093074.749293923.1671180305-1403019528.1663574162](#) (fecha de consulta: 22 de noviembre de 2022).

SINGHAL, B., DHAMEJA, G. & SEKHAR PANDA, P. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*, Apress, New York. Disponible en: https://link.springer.com/chapter/10.1007/978-1-4842-3444-0_2#Sec2 (fecha de consulta: 1 de marzo de 2022)

SKLAROFF, J. (2017). "Smart Contracts and the Cost of Inflexibility", *University of Pennsylvania Law Review*, Vol. 166, No. 1, pp. 263-303. Disponible en: <https://ssrn.com/abstract=3008899> (fecha: de consulta 1 de abril de 2020).

SPREY, J (2019.) "Blockchain and the controller under the GDPR: finding a necessary balance for BC to become a mainstream infrastructure". Disponible en: <https://www.vwsadvocaten.nl/en/blockchain-and-the-gdpr-data-controllers-and-data-processors/> (fecha de consulta: 24 de junio de 2022).

STARK, J. (2016). "Making Sense of Blockchain Smart Contracts". Disponible en: <https://www.coindesk.com/making-sense-smart-contracts> (fecha: de consulta 2 de febrero de 2020).

STEINBECK, D. (2028). "How New EU Privacy Laws Will Impact Blockchain: Expert Take". Disponible en: <https://cointelegraph.com/news/how-new-eu-privacy-laws-will-impact-blockchain-expert-take> (fecha de consulta: 9 de junio de 2022).

SUNG, S. (2021). "A new key protocol design for cryptocurrency wallet". *ICT Express*, Vol. 7, No. 3. Disponible en: <https://www.sciencedirect.com/science/article/pii/S2405959521000904> (fecha de consulta: 28 de agosto de 2022).

SURDEN, H. (2017). "Values Embedded in Legal Artificial Intelligence", *University of Colorado Law School Legal Studies Research Paper Series*, No. 17-17. Disponible en: <https://ssrn.com/abstract=2932333> (fecha de recuperación 20 de enero de 2020).

SUROWIECKI, J. (2005). *Cien mejor que uno: la sabiduría de la multitud o por qué la mayoría siempre es más inteligente que la minoría*, Tendencias.

SUROWIECKI, J. (2005). *The Wisdom Of Crowds: Why the Many are Smarter than the Few and How Collective Wisdom Shapes Business, Economics, Society and Nations*, Little Brown.

- SWAN M. (2016). "Blockchain Temporality: Smart Contract Time Specifiability with Blocktime", *Computer Science*, vol 9718, pp. 184-196. Disponible en: https://doi.org/10.1007/978-3-319-42019-6_12 (fecha: de consulta 4 de agosto de 2020).
- SZABO, N. (1997). "Formalizing and Securing Relationships on Public Networks", *First Monday*, Vol. 2, No. 9. Disponible en: <https://doi.org/10.5210/fm.v2i9.548> (fecha: de consulta 1 de abril de 2020).
- SZABO, N. (1996). "Smart Contracts: Building Blocks for Digital Markets". Disponible en: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (fecha de consulta: 16 de abril de 2020).
- SZABO, N. (1994). "Smart Contracts". Disponible en: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> (fecha de consulta: 16 de abril de 2020).
- TAKAHASHI, K. (2018). "Blockchain and Smart Contract for Contract Management (Dispute Prevention and Generation)". Disponible en: SSRN: <https://ssrn.com/abstract=3566678> (fecha de consulta: 17 de mayo de 2020).
- TAPSCOTT, D. & TAPSCOTT, A. (2017). *La revolución blockchain*, 4. Edición, Deusto, Barcelona.
- TATAR, U., GOKCE, Y., & NUSSBAUM, B. (2020). "Law versus technology: Blockchain, GDPR, and tough tradeoffs", *Computer Law & Security Review*, Vol. 38. Disponible en: <https://www.sciencedirect.com/science/article/abs/pii/S0267364920300595> (fecha de consulta: 23 de mayo de 2022).
- TAYLOR, S. K., ARIFFIN, A., ARIFFIN, K. A. Z., & ABDULLAH, S. (2021). "Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets", In *2021 3rd International Cyber Resilience Conference*. Disponible en <https://ieeexplore.ieee.org/abstract/document/9392446/authors#authors> (fecha de consulta: 28 de agosto de 2022).

- TEPERDJIAN, R. (2020). "The Puzzle of Squaring Blockchain with the General Data Protection Regulation", *jurimetrics*, Vol. 60, No. 3. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3638736 (fecha de consulta: 20 de junio de 2021).
- TEVENDALE, C. & MORGAN, C. (2018). "Blockchain and smart contracts: novel opportunities for improving efficiency in contract execution and dispute resolution". Disponible en: <https://www.herbertsmithfreehills.com/latest-thinking/blockchain-and-smart-contracts-novel-opportunities-for-improving-efficiency-in> (fecha de consulta: 10 de febrero de 2021).
- TJONG TJIN TAI, E. (2019). "Challenges of Smart Contracts", *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, (Dirs. DIMATTEO, L., CANNARSA, M. & PONCIBÒ, C.), Ed.: Cambridge University Press, Cambridge, pp. 80-101.
- TJONG TJIN TAI, E. (2018). "Force majeure and excuses in smart contracts", *Tilburg Private Law*, documento de trabajo, No. 10., pp. Disponible en: <http://dx.doi.org/10.2139/ssrn.3183637> (fecha de consulta: 10 de septiembre de 2020).
- TORRELLES-TOREA, E. (2021). "La resolución de los contratos por consumidores en tiempos de pandemia. Art. 36. 1 y 2 RD-ley 11/2020/", *Revista de Derecho Civil*, Vol. 8, No. 2, pp. 93-145. Disponible en: <https://www.nreg.es/ojs/index.php/RDC/article/view/635> (fecha de consulta: 2 de mayo de 2022).
- TRANTIS, G. (2002). "The Efficiency of Vague Contract Terms: A Response to The Schwartz-Scott Theory of U.C.C. Article 2", *Louisiana Law Review*, vol. 62, pp. 1065- 1079. Disponible en: <https://digitalcommons.law.lsu.edu/lalrev/vol62/iss4/4> (fecha de consulta: 2 de octubre de 2019).
- TROTTER, J.K. (2014). "Public NYC Taxicab Database Lets You See How Celebrities Tip". Disponible en: <https://www.gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546> (fecha de consulta: 5 de agosto de 2021).
- TSE, G. (2019). "Blockchain dispute resolution: a better alternative for the decentralised world?". Disponible en: <https://www.taylorvinters.com/article/blockchain-dispute->

- [resolution-a-better-alternative-for-the-decentralised-world](#) (fecha de consulta: 6 de febrero de 2021).
- TUCKER, P. (2013). Has big data made anonymity impossible?, *Technology Review*, Vol. 166, No. 4. Disponible en: <https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/> (fecha de consulta: 2 de agosto de 2022).
- TUR FAÚNDEZ, C. (2018). *Smart contracts: análisis jurídico*, Ed.: Reus, Madrid.
- ULPGC. (2015). “De Boole a Google: la lógica booleana en la vida cotidiana”. Disponible en: https://biblioteca.ulpgc.es/noticia_bicentenario_george_boole (fecha de consulta: 12 de febrero de 2021).
- UNIDROIT. (2016). “Principios Unidroit Sobre Los Contratos Comerciales Internacionales 2016”. Disponible en: <https://www.unidroit.org/wp-content/uploads/2021/06/Unidroit-Principles-2016-Spanish-bl.pdf> (fecha de consulta: 12 de junio de 2021).
- UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007). *Dictamen 4/2007 sobre el concepto de datos personales*. Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf (fecha de consulta: 17 de junio de 2021).
- UNIÓN EUROPEA, GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014). *Dictamen 05/2014 sobre técnicas de anonimización*. Disponible en <https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf> (fecha de consulta: 17 de junio de 2021).
- U.S. DEPARTMENT OF THE TREASURY (2022). *Crypto-Assets: Implications for Consumers, Investors, and Businesses*. Disponible en: https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf (fecha de consulta: 3 de octubre de 2022).
- VALPĪTERE, M. (2020). “*Right to erasure*” and private blockchain in the European Union: legal requirements and technical possibilities, Tesis de grado. Disponible en: https://dspace.lu.lv/dspace/bitstream/handle/7/52535/Valpitere_Marina.pdf?sequence=1 (fecha de consulta: 10 de mayo de 2022).

- VAN DER AUWERA E., SCHOUTENS W., PETRACCO GIUDICI M. & ALESSI L. (2020) "Blockchain", *Financial Risk Management for Cryptocurrencies*, (Dirs. VAN DER AUWERA E., SCHOUTENS W., PETRACCO GIUDICI M. & ALESSI L.), Ed.: Springer, Cham. pp. 3-17.
- VANEGAS – GOMEZ, A. (2016). "El camino hacia el ordenador cuántico: qubits y qudits". Disponible en: <https://www.bbvaopenmind.com/tecnologia/mundo-digital/el-camino-hacia-el-ordenador-cuantico-qubits-y-qudits/> (fecha de consulta: 1 de octubre de 2020).
- VANNIEUWENHUYSE, G. (2018). "Arbitration and New Technologies: Mutual Benefits", *Journal of International Arbitration*, Vol. 35, No. 1, pp. 119-129. Disponible en <https://bit.ly/2CggA8d> (Fecha de consulta: 5 de septiembre de 2019).
- VELASCO, J. (2014). "Mt.Gox y su hundimiento: pérdidas millonarias para unas de las referencias de Bitcoin". Disponible en: <https://hipertextual.com/2014/02/hundimiento-mt-gox> (fecha de consulta: 12 de septiembre de 2022).
- VERSTRAETE, M. (2019). "The Stakes of Smart Contracts", *Loyola University Chicago Law Journal*, Vol. 50, pp. 743-795. Disponible en: <https://ssrn.com/abstract=3178393> (fecha de consulta: 3 de febrero de 2020).
- VOIGT, P., & VON DEM BUSSCHE, A. (2017). *The EU general data protection regulation (GDPR). A Practical Guide*, Springer International Publishing, Cham, Switzerland
- VON WENDLAND, M. (2018). "Smart contracts that are smart and can function as legal contracts - A Review of Semantic Blockchain and Distributed Ledger Technologies". Disponible en: <https://arxiv.org/abs/1805.01279> (fecha de consulta: 7 de diciembre de 2020).
- WALCH, A. (2019). "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems", *Chapter in Crypto Assets: Legal and Monetary Perspectives*. Disponible en SSRN: <https://ssrn.com/abstract=3326244> (fecha de consulta: 10 de agosto de 2022).
- WEBER, R.H. (2018). "'Rose is a rose is a rose is a rose' – what about code and law?", *Computer Law & Security Review*, Vol. 34, No. 4, pp. 701-706. ISSN 0267-

3649. Disponible en: <http://www.sciencedirect.com/science/article/pii/S0267364918301882> (fecha de consulta: 2 de abril de 2019).
- WERBACH, K. (2018). "Trust, But Verify: Why the Blockchain Needs the Law", *Berkeley Technology Law Journal*, Vol. 33, No. 489, pp. 589-552 ISSN 1556-5068. Disponible en: <https://papers.ssrn.com/abstract=2844409> (fecha de consulta: 18 de julio de 2019).
- WERBACH, K. (2018). *The blockchain and the new architecture of trust*, The MIT Press, Cambridge, Massachusetts.
- WERBACH, K. (2018). "The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy", *Florida Law Review*, Vol. 69, pp. 887-957. Disponible en: doi:10.2139/ssrn.2732269 (fecha de consulta: 9 de diciembre de 2019).
- WERBACH, K. & CORNELL, N. (2017). "Contracts ex machina", *Duke law journal*, Vol. 67, No. 2, pp. 101-170 Disponible en: <https://ssrn.com/abstract=2936294> (fecha de consulta: 20 de agosto de 2019).
- WOODS, C. (2018). "Mind games", *Kluwer Mediation Blog*. Disponible en: <http://mediationblog.kluwerarbitration.com/2018/04/08/mind-games/> (fecha de consulta: 12 de abril de 2021).
- WONG, B. (2019). "Delimiting the concept of personal data after the GDPR", *Legal Studies*, Vol. 39, No. 3. pp. 517- 532. Disponible en: <https://www.cambridge.org/core/journals/legal-studies/article/abs/delimiting-the-concept-of-personal-data-after-the-gdpr/20758F3E090F79032F0A41C5843E82D9> (fecha de consulta: 16 de junio de 2021).
- WORLD ECONOMIC FORUM (2020). *Bridging the Governance Gap: Dispute resolution for blockchain-based transactions- White Paper*. Disponible en: <https://www.weforum.org/whitepapers/bridging-the-governance-gap-dispute-resolution-for-blockchain-based-transactions> (fecha de consulta: 3 de febrero de 2021).
- WP ENGINE. (2022). "Unmasked: What 10 million passwords reveal about the people who choose them". Disponible en: <https://wpengine.com/resources/passwords-unmasked-infographic/> (fecha de consulta: 10 de agosto de 2022).

- WRIGHT, A. & DE FILIPPI, P. (2015). "Decentralized Blockchain Technology and the Rise of Lex Cryptographia". Disponible en: <https://papers.ssrn.com/abstract=2580664> (fecha de consulta 16 de abril de 2019).
- WINNER, L. (1980). "Do Artifacts Have Politics?", *Daedalus*, Vol. 109, No. 1, pp. 121–136. Disponible en: <https://www.jstor.org/stable/20024652?origin=JSTOR-pdf&seq=1> (fecha de consulta: 2 de enero de 2020).
- YAGA, D., MELL, P., ROBY, N., & SCARFONE, K. (2019). *Blockchain technology overview*, National Institute of Standards and Technology, Gaithersburg. Disponible en: <https://doi.org/10.6028/NIST.IR.8202> (fecha de consulta: 7 de septiembre de 2021).
- YÉPEZ, M., VELA, M. & HARO, B. (2020). “Smart contracts y el arbitraje: hacia un modelo de justicia deslocalizado”, *USFQ Law Review*, Vol. 7, No. 1. Disponible en: <https://revistas.usfq.edu.ec/index.php/lawreview/article/view/1698> (fecha de consulta: 5 de febrero de 2021).
- YEUNG, K. (2019). "Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law", *The moder Law Review*, Vol. 82, No. 2. Disponible en: <https://ssrn.com/abstract=3347280> (Fecha de consulta: 25 de octubre de 2019).
- ZETZSCHE, D. A., ANNUNZIATA, F., ARNER, D. W., & BUCKLEY, R. P. (2021). “The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy”. *Capital Markets Law Journal*, Vol. 16, No. 2, pp. 203-225. Disponible en: <https://academic.oup.com/cmlj/article-abstract/16/2/203/6324188?redirectedFrom=fulltext> (fecha de consulta: 22 de septiembre de 2022).
- ZHENG, Z., XIE, S., DAI, H., CHEN, X., & WANG, H. (2017). “An overview of blockchain technology: Architecture, consensus, and future trends”, *IEEE international congress on big data (BigData congress)*. Disponible en: <https://ieeexplore.ieee.org/document/8029379> (fecha de consulta: 1 de noviembre de 2022).

Webgrafía

- “About Rhubarb”. (Sin fecha). Disponible en: https://www.rhucoin.com/about_rhu.aspx (fecha de consulta: 1 de marzo de 2021).
- “About Rhubarb”. (Sin fecha). Disponible en: https://www.rhucoin.com/about_rhu.aspx (fecha de consulta: 1 de marzo de 2021).
- “About us - JAMS Mediation, Arbitration and ADR Services”. (Sin fecha). Disponible en: <https://www.jamsadr.com/about/> (fecha de consulta: 20 de abril de 2020).
- “An Open Letter”. (2016). Disponible en: <https://pastebin.com/CcGUBgDG> (fecha de consulta: 18 de diciembre de 2019).
- “Aragon whitepaper”. (2019). Disponible en: <https://github.com/aragon/whitepaper> (fecha de consulta: 15 de febrero de 2021).
- “Arbitration library”. (2017). Disponible en: <https://codelegit.com/tag/arbitration-library/> (fecha de consulta: 21 de marzo de 2021).
- Ataques de máquina en medio “¿Qué son, y cómo podemos evitarlos?” (Sin fecha). Disponible en: https://www.internetsociety.org/wp-content/uploads/2020/12/Man-in-the-Middle-Fact-Sheet_final_ES.pdf (fecha de consulta: 22 de marzo de 2022).
- “Bamboo: a language for morphing smart contracts”. (Sin fecha). Disponible en: <https://github.com/pirapira/bamboo> (fecha de consulta: 11 de junio de 2020).
- “BankThink Smart Contracts Were Around Long Before Cryptocurrency”. (2016). Disponible en: <https://www.americanbanker.com/opinion/smart-contracts-were-around-long-before-cryptocurrency> (fecha de consulta: 17 de junio de 2020).
- “Blockchain and GDPR: beyond the right to be forgotten”. (2018). Disponible en: <https://www.osborneclarke.com/insights/blockchain-gdpr-beyond-right-forgotten> (fecha de consulta: 21 de junio de 2022).
- “Blockchains Privadas, Públicas y de Consorcios - ¿En qué se diferencian?”. (2021). Disponible en: <https://academy.binance.com/es/articles/private-public-and-consortium-blockchains-whats-the-difference>
- “Chainalysis”. (Sin fecha). <https://www.chainalysis.com/> (fecha de consulta: 1 de abril de 2022).

- “Cifrado asimétrico”. (Sin fecha). (2022). Disponible en: <https://www.ionos.es/digitalguide/servidores/seguridad/cifrado-asimetrico/> (fecha de consulta: 20 de mayo de 2022).
- “Ciphertrace”. (Sin fecha). Disponible en: <https://ciphertrace.com/> (fecha de consulta: 1 de abril de 2022).
- “Corda”. (Sin fecha). Disponible en: <https://corda.net/> (fecha de consulta: 10 de mayo de 2021)
- “Crowdsourcing: A Definition”. (Sin fecha). Disponible en: <https://crowdsourcing.typepad.com/cs/> (fecha de consulta: 1 de abril de 2021).
- “Cuentas de Ethereum”. (Sin fecha). (2022). Disponible en: <https://ethereum.org/es/developers/docs/accounts/> (fecha de consulta: 1 de abril de 2022).
- “Derecho al olvido o derecho de supresión”. (Sin fecha). Disponible en: <https://dpej.rae.es/lema/derecho-al-olvido-o-derecho-de-supresi%C3%B3n#:~:text=1.,2> (fecha de consulta 2 de junio de 2022).
- “Dispute lifecycle”. (Sin fecha). Disponible en: <https://documentation.aragon.org/products/aragon-court/dispute-lifecycle> (fecha de consulta: 16 de julio de 2021).
- “Elliptic”. (Sin fecha). Disponible en: <https://www.elliptic.co/> (fecha de consulta: 1 de abril de 2022).
- “Ethereum”. (Sin fecha). Disponible en: <https://ethereum.org/es/> (fecha de consulta: 10 de junio de 2020).
- Explanation of Terms and Disclaimer, The DAO”. (2016). Disponible en: <https://perma.cc/7QV6-HWUT> (fecha de consulta: 18 de diciembre de 2019).
- “Frequently asked questions”. (Sin fecha). Disponible en: <https://www.rhucoin.com/faq.aspx> (fecha de consulta: 15 de febrero de 2021).
- “GDPR Vs. Blockchain – Technology Against The Law”. Disponible en: <https://www.eurolatamlex.com/publications/news/42-gdpr-vs-blockchain-technology-against-the-law.html> (fecha de consulta: 10 de mayo de 2022).

“hyperledger”. (Sin fecha). Disponible en: <https://www.hyperledger.org/> (fecha de consulta: 10 de mayo de 2021).

“How Are Ricardian Contracts Different From Smart Contracts?”. (2021). Disponible en: <https://learn.bybit.com/defi/how-are-ricardian-contracts-different-from-smart-contracts/> (fecha de consulta: 3 de enero de 2022).

“Legal engineering is the practice of writing smart contracts that automate legally-enforceable rights and obligations”. (Sin fecha). Disponible en: https://github.com/monax/legacy-content/blob/master/learn/legal_engineering.md (fecha de consulta: 16 de mayo de 2020).

“Los grandes muros de seguridad que los países están construyendo en Internet”. (2016). Disponible en: <https://www.xataka.com/tecnologiazan/los-grandes-muros-de-seguridad-que-los-paises-estan-construyendo-en-internet> (fecha de consulta: 5 de enero de 2020).

“Meet the Open Justice Platform” (Sin fecha). Disponible en: <https://jur.io/products/open-justice/#:~:text=Open%20Justice%20Platform,are%20enforceable%20in%20166%20countries>. (fecha de consulta: 12 de marzo de 2022).

“Merklescience”. (Sin fecha). Disponible en: <https://www.merklescience.com/> fecha de consulta: 1 de abril de 2022).

“MONAX”. (Sin fecha). Disponible en: <https://monax.io/> (fecha de consulta: 20 de junio de 2020).

“Monax legacy content- What are Smart Contracts?”. (Sin fecha). Disponible en: https://github.com/monax/legacy-content/blob/master/learn/smart_contracts.md (fecha de consulta: 10 de junio de 2020).

“Monero” (Sin fecha). Disponible en: <https://www.getmonero.org/> (fecha de consulta: 10 de mayo de 2022).

“NXTER”. (Sin fecha). Disponible en: <https://www.nxter.org/understanding-nxt-cryptocurrency/> (fecha de consulta: 16 de junio de 2020).

“Non-fungible tokens (NFT)”. (Sin fecha). Disponible en: <https://ethereum.org/en/nft/> (fecha de consulta: 12 de septiembre de 2022).

Our Story”. (Sin fecha). Disponible en: <https://www.rhucoin.com/our-story.aspx> (fecha de consulta: 1 de marzo de 2021).

“PeopleClaim”. (Sin fecha). Disponible en: <https://www.peopleclaim.com/> (fecha de consulta: 27 de febrero de 2021).

“Pepper (cifrado)” (Sin fecha). Disponible en: <https://kripkit.com/pepper-cifrado/> (fecha de consulta: 10 de agosto de 2021).

“Pepper (criptografía)”. (Sin fecha). Disponible en: [https://hmong.es/wiki/Pepper \(cryptography\)](https://hmong.es/wiki/Pepper_(cryptography)) (fecha de consulta: 9 de agosto de 2021).

“PolyNetwork”. (Sin fecha). “ <https://www.poly.network/#/> (fecha de consulta: 12 de septiembre de 2022).

Principios De Derecho Europeo De Los Contratos”. (Sin fecha). Disponible en: <http://www.internationalcontracts.net/documentos-derecho-internacional/Principios-del-Derecho-Contractual-Europeo.pdf> (fecha de consulta: 12 de junio de 2021).

“Putting The Contracts in Smart Contracts”. (Sin fecha). Disponible en: <https://erisindustries.com/components/erislegal.html?redirect=true> (fecha de consulta: 3 de octubre de 2020).

“Qué es Bitcoin Core”. (2020). Disponible en: <https://academy.bit2me.com/que-es-bitcoin-core/> (fecha de consulta: 23 de mayo de 2021).

“¿Qué es el Hashing?” (2019). Disponible en: <https://academy.binance.com/es/articles/what-is-hashing> (fecha de consulta: 6 de agosto de 2021).

“¿Qué es Mt Gox?” (2022). Disponible en: <https://academy.bit2me.com/que-es-mt-gox/> (fecha de consulta: 17 de septiembre de 2022).

“¿Qué es RootStock o RSK?”. (Sin fecha). Disponible en: <https://academy.bit2me.com/que-es-rootstock-rsk/> (fecha de consulta: 1 de julio de 2020).

“¿Qué es una billetera de criptomonedas?”. (Sin fecha). Disponible en: <https://www.coinbase.com/es-LA/learn/crypto-basics/what-is-a-crypto-wallet> (fecha de consulta: 12 de septiembre de 2022).

- “¿Qué es un ataque de fuerza bruta? (Sin fecha) Disponible en: <https://www.avast.com/es-es/c-what-is-a-brute-force-attack#gref> (fecha de consulta: 5 de agosto de 2021).
- “¿Qué es un nodo? (2022). Disponible en: <https://academy.bit2me.com/que-es-un-nodo/> (fecha de consulta: 24 de julio de 2022).
- “¿Qué es un nodo Bitcoin?” (Sin fecha). Disponible en: <https://www.bitpanda.com/academy/es/lecciones/que-es-un-nodo-bitcoin/#que-es-un-nodo-de-luz> (fecha de consulta: 22 de julio de 2022).
- “¿Qué es un OP_CODE?”. (Sin fecha). Disponible en: <https://academy.bit2me.com/que-es-un-op-code/> (fecha de consulta: 16 de junio de 2020).
- “¿Qué hace que una Blockchain sea segura?” (2019). Disponible en: <https://academy.binance.com/es/articles/what-makes-a-blockchain-secure> (fecha de consulta: 6 de agosto de 2021).
- “¿Qué son las firmas de anillo?”. (2021). Disponible en: <https://crypto4dummy.com/que-son-las-firmas-de-anillo/> (fecha de consulta: 10 de mayo de 2022).
- “¿Qué son los nodos?” (2018). Disponible en: <https://academy.binance.com/es/articles/what-are-nodes> (fecha de consulta: 12 de julio de 2022).
- “Resolución de litigios en línea – acerca de la plataforma RLL”. (Sin fecha). Disponible en: <https://ec.europa.eu/consumers/odr/main/?event=main.home.howitworks> (fecha de consulta: 1 de marzo de 2021).
- “Resolución de litigios en línea- Organismos de resolución de litigios”. (Sin fecha). Disponible en: <https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.adr.show> (fecha de consulta: 13 de marzo de 2021).
- “Ricardian contracts: A smarter way to do smart contracts?”. (Sin fecha). Disponible en: <https://www.schoenherr.eu/publications/publication-detail/ricardian-contracts-a-smarter-way-to-do-smart-contracts/> (fecha de consulta: 17 de agosto de 2020).
- “Ricardian Contracts in OpenBazaar”. (Sin fecha). Disponible en: <https://gist.github.com/drwash0/a5380544c170bdbbbad8> (fecha de consulta: 17 de agosto de 2020).

RIPPLE”. (Sin fecha). Disponible en: <https://ripple.com/> (fecha de consulta: 16 de junio de 2020).

“Ring CT” (Sin fecha) Disponible en: <https://www.getmonero.org/es/resources/moneropedia/ringsignatures.html> (fecha de consulta 12 de mayo de 2022).

“Ring signature” (Sin fecha). Disponible en: <https://www.getmonero.org/es/resources/moneropedia/ringsignatures.html> (fecha de consulta: 15 de abril de 2022).

ROOTSTOCK”. (Sin fecha). Disponible en: <https://www.rsk.co/es/> (fecha de consulta: 16 de junio de 2020).

“Running A Full Node” (Sin fecha). Disponible en: <https://bitcoin.org/en/full-node#what-is-a-full-node> (fecha de consulta: 7 de octubre de 2022).

“R3” (Sin fecha). Disponible en: <https://www.r3.com/corda-platform/> (fecha de consulta: 16 de junio de 2020).

“Smart Contracts: ¿Qué son, ¿cómo funcionan y qué aportan?”. (Sin fecha). Disponible en: <https://academy.bit2me.com/que-son-los-smart-contracts/> (fecha de consulta: 10 de junio de 2020).

“Sintaxis”. (Sin fecha). Disponible en: <https://dle.rae.es/sintaxis> (fecha de consulta: 12 de enero de 2021).

“Solidity”. (Sin fecha). <https://docs.soliditylang.org/en/v0.8.17/> (fecha de consulta: 11 de junio de 2020).

“Solidity todos los recursos sobre el lenguaje de programación de los smart contracts”. (Sin fecha). Disponible en: <https://www.miethereum.com/smart-contracts/solidity/> (fecha de consulta: 10 de junio de 2020).

“Stealth addresses” (Sin fecha). Disponible en: <https://www.getmonero.org/es/resources/moneropedia/stealthaddress.html> (fecha de consulta: 17 de abril de 2022).

“Stealth Addresses – Que es y por qué la utiliza Monero?”. (2022). Disponible en: <https://satoshilov.com/stealth-addresses-que-es-y-por-que-la-utiliza-monero/> (fecha de consulta: 10 de mayo de 2022).

“Support the Bitcoin network by running your own full node”. (Sin fecha). Disponible en: <https://bitcoin.org/en/full-node#what-is-a-full-node> (fecha de consulta: 24 de julio de 2022).

“The Ethereum Virtual Machine”. (Sin fecha). Disponible en: <https://docs.soliditylang.org/en/v0.6.11/introduction-to-smart-contracts.html#the-ethereum-virtual-machine> (fecha de consulta: 10 de junio de 2020).

“Vyper”. (Sin fecha) Disponible en: <https://vyper.readthedocs.io/en/stable/> (fecha de consulta: 11 de junio de 2020).

“What Is Gas?”. (2020). Disponible en: <https://support.mycrypto.com/general-knowledge/ethereum-blockchain/what-is-gas> (fecha de consulta: 25 de junio de 2020).

“What is mining?”. (Sin fecha). Disponible en: <https://www.coinbase.com/es/learn/crypto-basics/what-is-mining> (fecha de consulta: 1 de julio de 2022).

“Zcash”. (Sin fecha). Disponible en: <https://z.cash/> (fecha de consulta: 10 de mayo de 2022).

“@VitalikButerin”. (2018). Disponible en: <https://twitter.com/VitalikButerin/status/1051160932699770882> (fecha de consulta: 29 de junio de 2020).

Recursos multimedia

SÁENZ DE CABEZÓN, E. [Derivando]. (2018). “¿Cuál es la mejor forma de pagar la cena? la teoría de juegos”, archivo de video. Disponible en: https://www.youtube.com/watch?v=HxGvzia2PcU&ab_channel=Derivando (fecha de consulta: 12 de diciembre de 2022).

Anexo de jurisprudencia

CORTE DE APELACIONES DE LA REPUBLICA DE SINGAPUR. (2019) Caso Quoine Pte Ltd v B2C2 Ltd. Sentencia de 24 de febrero de 2020. Disponible en: <https://tinyurl.com/y5r6w9sd> (fecha de consulta: 1 de diciembre de 2020).

STS, Sala 1ª, 820/2013, de 17 de enero. *Contrato de compraventa de vivienda. Resolución de contrato. Rebus sic stantibus.*

STS, Sala 4ª, 1969/1997, de 22 de diciembre. *Recurso de casación para la unificación de doctrina. Reclamación de prestaciones.*

STJUE, Sala 1ª, 10 de diciembre de 2020, Asto: C-620/19, Land Nordrhein-Westfalen/ D.-H. T, EU:C:2020:649. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-620/19&language=ES> (fecha de consulta: 1 de junio de 2021).

STJUE, Sala 1ª, 10 de diciembre de 2020, Asto: C-620/19, Land Nordrhein-Westfalen/ D.-H. T, EU:C:2020:649. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-620/19&language=ES> (fecha de consulta: 1 de junio de 2021).

STJUE, Sala 3ª, de 9 de junio de 2020, Asto: C-272/19, VQ / Land Hessen EU:C:2020:53. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-272/19> (fecha de consulta: 10 de junio de 2021).

STJUE, Gran Sala, de 5 de junio de 2018, Asto: C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein y Wirtschaftsakademie Schleswig-Holstein GmbH/ Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht EU:C:2018:388. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210> (fecha de consulta: 29 de julio de 2022).

STJUE, Sala 2ª, de 20 de diciembre de 2017, Asto: C-434/16, Peter Nowak / Data Protection Commissioner, EU:C:2017:582. Disponible en: <https://curia.europa.eu/juris/liste.jsf?num=C-434/16> (fecha de consulta: 2 de junio de 2021).

STJUE, Sala 2ª, de 13 de mayo de 2014, Asto: C-131/12, Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, EU:C:2014:317. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12> (fecha de consulta: 5 de junio de 2022).

STJUE, Sala 2ª, de 19 de octubre de 2016, Asto: C-582/14, Patrick Breyer/ Bundesrepublik Deutschland, EU:C:2016:779. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-582/14&td=ALL> (fecha de consulta: 15 de junio de 2020).

STJUE, Sala 3ª, de 24 de noviembre de 2011, Asto: C-70/10, Scarlet Extended SA/ Soci  t   belge des auteurs, compositeurs et   diteurs SCRL (SABAM), EU:C:2011:771. Disponible en: <https://curia.europa.eu/juris/liste.jsf?language=es&jur=C,T,F&num=C-70/10&td=ALL> (fecha de consulta 10 de abril de 2022).

Anexo de legislaci  n

Espa  a

Espa  a. Circular 1/2022, de la Comisi  n Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados como objeto de inversi  n. *Bolet  n Oficial del Estado*, 10 de enero de 2022.

Espa  a. Real Decreto-ley 7/2021 de prevenci  n del blanqueo de capitales y de la financiaci  n del terrorismo. *Bolet  n Oficial del Estado*, 27 de abril de 2021

Espa  a. Real Decreto-ley 5/2021 de medidas extraordinarias de apoyo a la solvencia empresarial en respuesta a la pandemia de la COVID. *Bolet  n Oficial del Estado*, 12 de marzo de 2021.

Espa  a. Real Decreto-ley 11/2020, por el que se adoptan medidas urgentes complementarias en el   mbito social y econ  mico para hacer frente al COVID-19, *Bolet  n Oficial del Estado*, 31 de marzo de 2020.

Espa  a. Real Decreto Legislativo 4/2015, por el que se aprueba el texto refundido de la Ley del Mercado de Valores. *Bolet  n Oficial del Estado*, 23 de octubre de 2015.

Espa  a. Ley 10/2010 de prevenci  n del blanqueo de capitales y de la financiaci  n del terrorismo. *Bolet  n Oficial del Estado*, 28 de abril de 2010.

Espa  a. Real Decreto 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. *Bolet  n Oficial del Estado*, 16 de noviembre de 2007.

Espa  a. Ley 34/2002, de servicios de la sociedad de la informaci  n y de comercio electr  nico, *Bolet  n Oficial del Estado*, 11 de julio de 2002.

Espa  a. Ley 7/1998, sobre condiciones generales de la contrataci  n. *Bolet  n Oficial del Estado*, 13 de abril de 1998.

España. Real Decreto de 24 de julio de 1889, por el que se publica el Código Civil. *Boletín Oficial del Estado*, 16 de agosto de 1889.

Europa

Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE

Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado.

Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo de 14 de junio de 2017 sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE.

Reglamento (UE) 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) nº 2006/2004 y la Directiva 2009/22/CE.

Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE.

Propuesta de Reglamento Del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937.

Otros países

Malta. Cap. 590, Virtual Financial Assets Act, noviembre de 2018.

Francia. LOI No. 2019-486, relative à la croissance et la transformation des entreprises, mayo de 2019.