

AGUSTÍN MADRID PARRA

Director

MARÍA JESÚS BLANCO SÁNCHEZ

Coordinadora

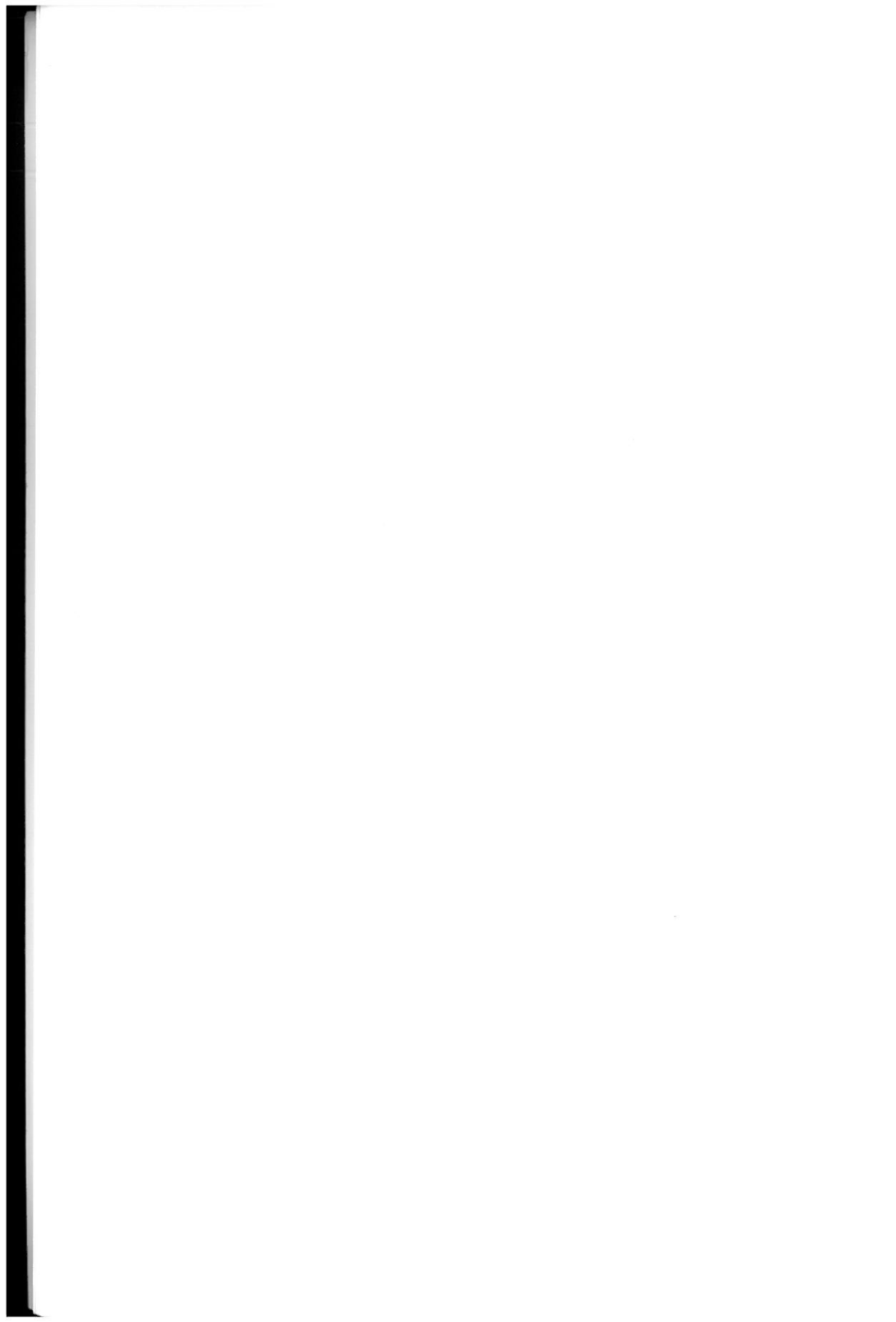
DERECHO MERCANTIL Y TECNOLOGÍA

Lucía Alvarado Herrera
Juan Arpio Santacruz
Nicolás Augoustatos Zarco
Moisés Barrio Andrés
Zofia Bednarz
Antonio David Berning Prieto
María Jesús Blanco Sánchez
José María Botello Hermosa
Consuelo Camacho Pereira
Fernando Carbajo Cascón
María Isabel Carmona González
Antonio Casado Navarro
José Antonio Castillo Parrilla
Diego Cruz Rivero
Marina Echebarría Sáenz
Jorge Feliú Rey
Marta Fernández Cabrera
Carmen Rocío Fernández Díaz
Juan Flaquer Riutort
Antonio Francisco Galacho Abolafio
Marta García Mandaloniz
M. Esperança Ginebra Molins

María Gómez Santos
Pedro Mario González Jiménez
Marta Grande Sanz
Josep Gunnar Horrach Armo
Patricia Llopis Nadal
Agustín Madrid Parra
Apol•Lònia Martínez Nadal
Antonio Merchán Murillo
Joaquín José Noval Lamas
Mayte Otero Cobos
M^a Del Carmen Pastor Sempere
Ángela María Pérez Rodríguez
Isabel Ramos Herranz
Juan Francisco Rodríguez Ayuso
Juan Pablo Rodríguez Delgado
Teresa Rodríguez De Las Heras Ballell
José Ruiz Espinosa
Ana Sánchez Rubio
Marc Simon Altaba
José Carlos Vázquez Cueto
Trinidad Vázquez Ruano
José Antonio Vega Vega

THOMSON REUTERS

ARANZADI



AGUSTÍN MADRID PARRA

Director

MARÍA JESÚS BLANCO SÁNCHEZ

Coordinadora

DERECHO MERCANTIL Y TECNOLOGÍA

Lucía Alvarado Herrera

Juan Arpio Santacruz

Nicolás Augoustatos Zarco

Moisés Barrio Andrés

Zofia Bednarz

Antonio David Berning Prieto

María Jesús Blanco Sánchez

José María Botello Hermosa

Consuelo Camacho Pereira

Fernando Carbajo Cascón

María Isabel Carmona González

Antonio Casado Navarro

José Antonio Castillo Parrilla

Diego Cruz Rivero

Marina Echebarría Sáenz

Jorge Feliú Rey

Marta Fernández Cabrera

Carmen Rocío Fernández Díaz

Juan Flaquer Riutort

Antonio Francisco Galacho Abolafio

Marta García Mandaloniz

M. Esperança Ginebra Molins

María Gómez Santos

Pedro Mario González Jiménez

Marta Grande Sanz

Josep Gunnar Horrach Armo

Patricia Llopis Nadal

Agustín Madrid Parra

Apol•Lònia Martínez Nadal

Antonio Merchán Murillo

Joaquín José Noval Lamas

Mayte Otero Cobos

M^a Del Carmen Pastor Sempere

Ángela María Pérez Rodríguez

Isabel Ramos Herranz

Juan Francisco Rodríguez Ayuso

Juan Pablo Rodríguez Delgado

Teresa Rodríguez De Las Heras Ballell

José Ruiz Espinosa

Ana Sánchez Rubio

Marc Simon Altaba

José Carlos Vázquez Cueto

Trinidad Vázquez Ruano

José Antonio Vega Vega

THOMSON REUTERS

ARANZADI

Primera edición, 2018



THOMSON REUTERS PROVIEW® eBooks

Incluye versión en digital

El editor no se hace responsable de las opiniones recogidas, comentarios y manifestaciones vertidas por los autores. La presente obra recoge exclusivamente la opinión de su autor como manifestación de su derecho de libertad de expresión.

La Editorial se opone expresamente a que cualquiera de las páginas de esta obra o partes de ella sean utilizadas para la realización de resúmenes de prensa.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra (www.conlicencia.com; 91 702 19 70 / 93 272 04 45).

Por tanto, este libro no podrá ser reproducido total o parcialmente, ni transmitirse por procedimientos electrónicos, mecánicos, magnéticos o por sistemas de almacenamiento y recuperación informáticos o cualquier otro medio, quedando prohibidos su préstamo, alquiler o cualquier otra forma de cesión de uso del ejemplar, sin el permiso previo, por escrito, del titular o titulares del copyright.

Thomson Reuters y el logotipo de Thomson Reuters son marcas de Thomson Reuters

Aranzadi es una marca de Thomson Reuters (Legal) Limited

© 2018 [Thomson Reuters (Legal) Limited / Agustín Madrid Parra (Dir.) y María Jesús Blanco Sánchez (Coord.)]

© Portada: Thomson Reuters (Legal) Limited

Editorial Aranzadi, S.A.U.

Camino de Galar, 15

31190 Cizur Menor (Navarra)

ISBN: 978-84-9099-214-2

DL NA 1385-2018

Printed in Spain. Impreso en España

Fotocomposición: Editorial Aranzadi, S.A.U.

Impresión: Rodona Industria Gráfica, SL

Polígono Agustinos, Calle A, Nave D-11

31013 – Pamplona

Índice General

Página

PRÓLOGO	41
---------------	----

PARTE I

NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

CAPÍTULO 1

REFLEXIONES SOBRE LA ELECTRONIFICACIÓN DE LAS INSTITUCIONES MERCANTILES: HACIA UNA RECONSTRUCCIÓN DE LA TEORÍA JURÍDICA	53
--	-----------

JOSE ANTONIO VEGA VEGA

I. El fenómeno de la electronificación	54
II. Las especialidades del documento electrónico	57
III. La contratación electrónica	59
1. <i>Problemática actual</i>	59
2. <i>Distinción entre comercio electrónico y contratación electrónica</i>	62
3. <i>La cuestión de la naturaleza jurídica del contrato electrónico</i>	63
IV. Las instituciones electrónicas como nueva realidad jurídica	64
V. La lex electrónica	68
1. <i>Los instrumentos electrónicos en el ámbito internacional</i>	68
2. <i>Normativa europea sobre electronificación de documentos</i>	72
3. <i>Disposiciones europeas sobre transacciones efectuadas mediante instrumentos electrónicos de pagos</i>	76

dinero electrónico⁷². En concreto, quedó probado que a pesar de haber optado la entidad por el método de salvaguarda previsto en el artículo 10.1.a) LSP, de las diez cuentas que tenía la entidad sólo cuatro de ellas (que además representaban un importe residual del total de los fondos que debían ser garantizados) se consideraron válidas como método de salvaguarda, ya que el resto no cumplía con los requisitos de ser cuentas separadas y exclusivas para la actividad de dinero electrónico y no contaban con la mención especial «saldos de clientes de entidades de dinero electrónico» [requisito éste exigido para los depósitos a la vista en el artículo 16.2.a) RD 778/2012]. Además, también se puso de manifiesto que la entidad no había incluido en los contratos celebrados con los clientes mención alguna al procedimiento de salvaguarda, con incumplimiento de lo previsto en el artículo 16.1.a) RD 778/2012.

72. Nos referimos al caso que afectó a la entidad de dinero electrónico «Yunique money, EDE», a la que el Banco de España, por medio de Resolución del Consejo de Gobierno de 28 de marzo de 2015, impuso una serie de sanciones por la comisión de diversas infracciones. Además de la mencionada en el texto, la entidad de dinero electrónico presentaba deficiencias en la organización administrativa y contable, incumplía las normas relativas al nivel de recursos mínimos, y llevaba la contabilidad con irregularidades esenciales que impedían conocer su situación patrimonial y financiera. Tras la imposición de las sanciones, «Yunique money EDE» recurrió en alzada. Tras ser desestimado en alzada, recurrió a la Audiencia Nacional, que falló contra la entidad [vid. SAN de 20 de enero de 2016 (RJCA 2016 2002)].

Capítulo 10

Smart contracts y problemas jurídicos de los pagos con tecnologías blockchain*

Smart contracts and legal problems of payments with blockchain technologies

MARINA ECHEBARRÍA SÁENZ

*Profesora Titular de D^o Mercantil.
Acreditada a Cátedra de Derecho Mercantil.
Universidad de Valladolid.*

SUMARIO: I. LOS SMART CONTRACT O CONTRATOS AUTO EJECUTABLES. II. RÉGIMEN LEGAL DE LOS SMART CONTRACT. III. EL PROBLEMA DEL PAGO ELECTRÓNICO AUTOMÁTICO COMO FORMA DE EJECUCIÓN DE LOS SMART CONTRACT: DINERO ELECTRÓNICO Y CRIPTO MONEDAS VIRTUALES. 1. *La aparición de las criptomonedas virtuales con tecnología Blockchain; el ejemplo del Bitcoin.* 2. *La Tecnología de la cadena de bloques: funcionamiento de los registros compartidos o distributive ledger.* 3. *Secreto y criptografía de seguridad en Bitcoin.* 4. *Análisis de riesgos particulares y sistémicos del Bitcoin.* 4.1. *Riesgos individuales en Bitcoin.* 4.2. *Riesgos sistémicos de Bitcoin.* IV. RÉGIMEN JURÍDICO DE LAS OPERACIONES EN CRIPTOMONEDAS VIRTUALES. 1. *Hacienda Pública.* 2. *Normativa de prevención del blanqueo de capitales.* 3. *Normativa de servicios de pago.* 4. *Normativa del mercado de valores.* 5. *Régimen jurídico de los pagos en criptomonedas virtuales.* V. CONCLUSIONES. VI. BIBLIOGRAFÍA Y REFERENCIAS WEB.

* Este trabajo se inserta dentro de las labores del proyecto de investigación del Ministerio de Economía y Competitividad, DER2014-58744-R «Competencia y Distribución: nuevos retos en la sociedad globalizada y en contextos de crisis económica», bajo la dirección de las profesoras ECHEBARRÍA SÁENZ, Marina y HERRERO SUÁREZ, Carmen.

Resumen: Los contratos autoejecutables en formato electrónico son la culminación de la progresiva automatización de los procesos vinculados a las cadenas de valor. Una vez establecido el principio de equivalencia entre los formatos electrónicos y materiales, es posible reconstruir sin grandes dificultades su régimen jurídico. La mayor dificultad reside, sin embargo, en la obtención de sistemas de pago automatizados y aquí la tecnología de bloques ha irrumpido en el panorama jurídico con monedas virtuales como el Bitcoin que, si bien aportan grandes funcionalidades, nos plantean dudas en la aplicación de las estructuras normativas vigentes.

Palabras clave: contratos auto ejecutables, moneda virtual, Bitcoin, Blockchain, sistemas de pago, valores, sistemas descentralizados, sistemas disruptivos.

Abstract: Smart contracts or self-executing contracts in electronic format are the culmination of the progressive automation of processes linked to value chains. Once the principle of equivalence between electronic and material formats has been established, it is possible to build up their legal regime without great difficulties. The biggest difficulty lies, however, in obtaining automated payment systems and here the Blockchain technology has broken into the legal landscape with virtual currencies such as Bitcoin that, although provide great functionalities, raise doubts in the application of current regulatory structures

Keywords: smart contract, auto-executable contracts, virtual currency, Bitcoin, Blockchain, payment systems, values, decentralized systems, disruptive systems

I. LOS SMART CONTRACT O CONTRATOS AUTO EJECUTABLES

Los llamados Smart Contracts, pueden ser definidos como contratos en formato electrónico y de carácter autoejecutable. Toda su «inteligencia» reside en el hecho de que todas o alguna de las cláusulas del contrato son transcritas del lenguaje natural al lenguaje binario y convertidas en scripts o pequeños programas que se autoejecutarán ante un evento pre programado. Así, por ejemplo, si un documento de trazabilidad¹ indica que la mercancía ha salido de un almacén, el mensaje remitido a un ordenador liberará el pago por la entrega. Las tareas programadas pueden ser muy sencillas (emitir un voto), más complejas (efectuar un pago), o representar negocios jurídicos complejos como liberar una subvención, conceder un préstamo, liberar garantías o depósitos, etc. etc.² Llamo la atención sobre el factor de autoejecutabilidad: las cláusulas transcritas a código de programación implican un programa de ejecución. Se definen las reglas y las consecuencias de las mismas, lo mismo que en cualquier otro contrato que define

1. ECHEBARRÍA SÁENZ, J. A «La carta de porte emitida electrónicamente» en *Comentarios a la ley de transporte terrestre*, DUQUE DOMÍNGUEZ, J/MARTÍNEZ SANZ, F. (Dir.) Aranzadi Thomson-Reuters, Pamplona 2010, págs. 185-212
2. Véase http://opentransactions.org/wiki/index.php/Voting_Pools. ECHEBARRÍA SÁENZ, M., «Contratos electrónicos autoejecutables (Smart contract) y pagos con tecnología Blockchain» en *Revista de Estudios Europeos*, número monográfico Economía colaborativa, 2, diciembre 2017, ISSN: 2530-9854. <http://www.ree-uva.es/> pág. 67

obligaciones, pero esta vez, la diferencia reside en que una vez fijadas las pautas de ejecución estas son inmodificables e indisponibles por la voluntad de las partes, lo que asegura fiabilidad al buen fin del contrato.

El contrato autoejecutable es el resultado lógico del creciente proceso de automatización que ha ido dominando las cadenas de valor comerciales en el último decenio. Tomando como ejemplo más señalado la distribución comercial, primero se automatizó el tratamiento de las mercancías en almacén y su clasificación (etiquetado magnético), después se crearon los sistemas de producción a demanda automatizados o «just in time», finalmente se adhirieron al sistema comercial los documentos de trazabilidad de las mercancías y la comercialización a distancia por medios telemáticos (comercio electrónico) o en mercados electrónicos (e-markets). El uso de instrumentos de pago electrónico a distancia ha ido creciendo igualmente de forma exponencial, por lo que ya sólo quedaba cerrar el círculo y automatizar la propia realización de los contratos. El sistema, por otro lado, es susceptible de aplicarse a cualquier contexto de la contratación y por lo tanto tiene un desarrollo potencial enorme.

Aunque existe tendencia a identificar los Smart Contract con formatos que usan la tecnología de bloques (Blockchain), lo cierto es que conforme a un patrón de neutralidad tecnológica podemos considerar como Smart Contract a cualquier acuerdo que cumpla esta pauta usando otra fórmula tecnológica. Ocurre, sin embargo, que para que esta respuesta automática sea posible es necesario poder programar un pago que no dependa de una orden posterior a la ejecución de parte y es por esto que buena parte de los Smart Contract terminan apoyándose en la tecnología de bloques y ejecutando el pago en criptomonedas o monedas virtuales como el Bitcoin³.

La gran ventaja de los Smart Contracts es que sus scripts son susceptibles de programarse en serie con sencillez al almacenarse en una cadena de bloques o en protocolos compartidos por redes de ordenadores. Los contratos autoejecutables presentan evidentes ventajas, pues, una vez superada la complejidad inicial de la programación, operan de manera sencilla, rápida, inmodificable, con ejecución asegurada al no permitir el arrepentimiento y con la ventaja de que la operativa puede ser totalmente automatizada, incluida la perfección de los contratos sucesivos al contrato marco, lo que permite que sea una solución para el llamado internet de las cosas o para la economía digital automatizada que opera sin personas⁴.

3. La identificación de las monedas virtuales, criptomonedas o criptodivisas como tal es término habitual en toda la literatura financiera.

<http://ojphi.org/ojs/index.php/fm/article/view/548/469>

4. La concepción de la empresa o fábrica que no nos necesita se atribuye a Gill y Pratt en 2008. Sobre esta base, visionarios como Vitali Buterin creador de ethereum en 2014 (www.ethereum.org), defienden el uso de tecnologías blockchain para la creación de Organizaciones autónomas descentralizadas (DAOs). Véase SWARTZ, LANA, «El sueño del Blockchain. Imaginando alternativas tecnoeconómicas más allá del bitcoin» en CASTELLS, M. et al. *Otra economía es posible. Cultura y economía en tiempos de crisis*. Alianza editorial, Madrid, 2017, págs. 123-155.

II. RÉGIMEN LEGAL DE LOS SMART CONTRACT

¿Plantean alguna duda de legalidad los Smart Contract? Personalmente diría que aportan alguna dificultad, pero que todas ellas son salvables. Atendiendo al principio de libertad de forma (art. 51 C.Co.), que el consentimiento, objeto y causa de un contrato (art. 1261.C.) se plasme en formato digital, código binario de unos y ceros susceptibles de ejecución por una máquina, no le resta ninguno de los elementos necesarios para su validez legal atendiendo al principio de equivalencia funcional entre los medios de expresión físicos y los digitales que se recoge en el art. 3 n.º 6, 7 y 8 de la ley 59/2003 de firma electrónica y el art. 326 de la ley de enjuiciamiento civil.

Es cierto que el común de los humanos no somos capaces de interpretar directamente un código binario, pero no es menos cierto que poseemos máquinas para descifrarlos, y que podemos pactar simultáneamente los elementos del contrato en lenguaje humano y en lenguaje binario, de forma que se salven los posibles errores en el consentimiento. De hecho, en determinados contratos será necesaria la plasmación en lenguaje humano o natural de los términos del contrato autoejecutable para salvar el consentimiento de la parte, como ocurrirá necesariamente siempre que haya un consumidor implicado o si no existe una percepción directa de las cláusulas secundarias en cualquier contrato. En los contratos de ejecución automática perfeccionados y ejecutados por robots, sin embargo, tanto el programador de la oferta como el programador de la aceptación tienen ocasión de comprender y transmitir al titular responsable de la obligación el contenido de las prestaciones comprometidas y por ello el propio diseño del programa implicará el consentimiento de las partes, salvo aplicación de cláusulas sorpresivas o modificación unilateral de los scripts de ejecución. Incluso en una contratación completamente automatizada, es necesario recordar que las máquinas, hoy por hoy, no son susceptibles de manifestación de consentimiento alguno. Detrás de un proceso de contratación automatizado siempre está el hombre que organiza el sistema de concertación y prepara el programa, momento en el que se manifiesta el consentimiento humano en el proceso, directamente o por ejecución delegada del titular.

Finalmente, es cierto que en caso de discrepancia entre el script o programa de ejecución y los términos pactados en lenguaje humano, siempre se deberá dar prioridad a este último, que es el que finalmente recaba la manifestación de voluntad requerida por nuestro ordenamiento (art. 1261 C.C.), la manifestada por un ser humano, pero una vez manifestado el consentimiento, el pacto es susceptible de automatización y repetición estandarizada como contrato marco, y que la totalidad de los procesos de ejecución pueden ser automatizados sin reparo legal. El problema más evidente es el de la existencia de un posible error por diferencia entre la voluntad manifestada en el proceso de expresión en lenguaje natural y la ejecución contractual correspondiente al proceso expresado en lenguaje binario. Error que ha de ser de imposible percepción para el contratante o de difícil percepción para el experto que articula el sistema automatizado, en su nombre o por su cuenta, para que podamos hablar de la existencia de un error obstativo (art. 1265 C.C.) invalidante del negocio. Doctrina esta última que en nuestro país es muy restrictiva, y

nos lleva a considerar que la no percepción directa de consecuencias secundarias del contrato concertado entre empresarios no implicará automáticamente la nulidad o anulabilidad del contrato, si acaso nulidades parciales del negocio (art. 1300 C.C.), mientras que la falta de percepción por el consumidor de aspectos que deben ser detallados necesariamente por la normativa tutelar, como el precio completo incluidos conceptos indirectos, plazos de ejecución, condiciones de entrega etc. etc. se verían claramente sometidos al mandato tutelar del texto refundido de la ley de defensa de los consumidores y usuarios.

¿Constituye un problema la renuncia a la *exceptio non adimpleti contractus*, es decir, el carácter autoejecutable? Podría parecer que sí, ya que, en nuestros códigos, frente al incumplimiento de una parte cabe la excepción de incumplimiento, pero analizada convenientemente la situación, la respuesta es negativa: la ejecución automática es una respuesta a un evento desencadenante que implica el cumplimiento por la contraparte de aquello que se ha considerado relevante. Lo único a lo que se renuncia en el sistema es al «derecho a incumplir» y este no se haya consagrado en nuestro sistema legal. Si podemos pactar cláusulas penales y sistemas de ejecución reforzados, ¿Qué ha de impedirnos pactar un sistema que no nos permite incumplir una vez que la contraparte ha cumplido conforme a parámetros pre establecidos y libremente convenidos?

¿Plantea alguna duda el régimen legal en cuanto al momento del consentimiento, lugar de celebración, ley aplicable etc. etc.? Pues no, un contrato autoejecutable sigue las reglas generales de cualquier contrato concertado por vía electrónica, por lo que a falta de pacto o de foro y norma imperativa por protección del consumidor:

- Se entenderá concertado conforma a la regla del 1.262 C.C. y 50 C.Co., en el domicilio del oferente.
- Seguirá la regla del art. 54 C.Co en lo referente el momento de la perfección a efectos de fijación de la ley aplicable, de la capacidad de las partes y del cumplimiento o incumplimiento puntual.
- Seguirá comúnmente las reglas de los arts. 333 y 334 C.Co. para la transmisión del riesgo.
- Seguirá lo dispuesto en el art. 3 del Reglamento Roma I en lo tocante a ley aplicable⁵: En el mismo se consagra la autonomía de la voluntad como

5. Reglamento (CE) n. 593/2008 del Parlamento Europeo y del Consejo de 17-6-2008 sobre ley aplicable a las obligaciones contractuales. Véase, CALVO CARAVACA, A./CARRASCOSA GONZÁLEZ, J. «Problemas de extraterritorialidad en la contratación electrónica» en ECHEBARRÍA SÁENZ, J. (Dir) *El comercio electrónico*, págs. 145-217. VICENTE BLANCO, D.J. «Problemas de jurisdicción competente y ley aplicable en los mercados electrónicos» en VELASCO, ECHEBARRÍA, HERRERO (Dir) *Acuerdos horizontales, mercados electrónico y otras cuestiones actuales de competencia y distribución*, Valladolid, Lex Nova Thomsom-Reuters, 2014, págs. 644-666. Y del mismo «medios electrónicos de pago y jurisdicción competente en supuesto de contratos transfronterizos en Europa», en MATA MÁRTÍN, R./JAVATO MARTÍN, A. *Los medios electrónicos de pago*, págs. 270-319.

primera opción, no existiendo pacto, el art. 4 b señala la ley del Estado de residencia habitual del prestador de servicio, aunque el reglamento admite cláusulas de escape por existencia de vínculos más cercanos con el caso, y aquí en especial la opción del consumidor por acogerse a la normativa tutelar propia. En materia de compraventa, sin embargo, en defecto de pacto (art. 3), caben diversas posibilidades según se entienda que es una compraventa general (art. 4); ley del Estado del vendedor, un contrato de distribución; ley de residencia habitual del distribuidor, o venta mediante subasta; ley del prestador del servicio de subastas. Si es compraventa de servicios financieros se aplicará la ley del Estado del mercado (art. 4.1.h). En los supuestos de carácter mixto se aplicará la ley del Estado de residencia habitual de quien deba realizar la prestación característica del contrato (art. 4.2) pero siempre existirá cláusula de escape (art. 4.3) si el contrato presenta vínculos más estrechos con un ordenamiento distinto.

- Se aplicará lo dispuesto en los reglamentos Bruselas I⁶ y Bruselas I bis⁷ a efectos de fijación de jurisdicción en los casos con componente Internacional. A saber: libre elección de foro por elección expresa o sumisión tácita (sin paralización por excepción de Litis pendencia), y en su defecto será competente el juez del domicilio del demandado o del lugar de ejecución de la obligación (como foro de ataque). En materia de compraventa, sin embargo, Bruselas I Bis consagra el principio de «fortaleza europea» que protege a los domiciliados en la UE frente a demandas del exterior, protegiendo de la ejecución de sentencias extranjeras y permitiendo la demandar en la UE a domiciliados extranjeros o la aplicación de foro exorbitantes, mientras que si resulta aplicable la Convención de Viena de 1980, esta resulta de aplicación prioritaria sobre las normas conflictuales anteriores.

Así las cosas, el único problema reseñable es, por un lado el de solventar el cómo de la constitución de un contrato electrónico, para lo que existen múltiples compañías que aportan el bagaje técnico⁸, y el de completar la totalidad de la operación por medios electrónicos, ya que de otro modo, solo automatizaríamos una parte del proceso y siempre, finalmente, dependeríamos de la voluntad de cumplir de la contraparte si esta puede paralizar o bloquear la respuesta. El problema

-
6. Reglamento (CE) n. 44/2001 del Consejo de 22-12-2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
 7. Reglamento UE n. 1215/2012 del Parlamento Europeo y del Consejo de 12-12-2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
 8. Como ejemplos: BitHalo (<https://bithalo.org/>), BlackHalo (<http://blackhalo.info/>), Codiús (<https://codius.org/>) Counterparty (<http://counterparty.io/>) Rootstock (<https://www.oroynfinanzas.com/2015/10/rootstock-contratos-inteligentes-smart-contracts-ethereum-bitcoin/>) Ethereum (<https://www.oroynfinanzas.com/2015/07/ethereum-proyecto-bitcoin-2-0-mas-ambicioso-lanza-plataforma-descentralizada-frontier/>) (www.ethereum.org)

más evidente en este campo es el de asegurar un pago, por medios electrónicos, automatizado.

III. EL PROBLEMA DEL PAGO ELECTRÓNICO AUTOMÁTICO COMO FORMA DE EJECUCIÓN DE LOS SMART CONTRACT: DINERO ELECTRÓNICO Y CRIPTO MONEDAS VIRTUALES

Desde que la humanidad abandonó el trueque para adoptar el dinero como signo o medio de cambio, unidad de valor y sistema de medida de las cosas, éste y los restantes medios de cambio han sufrido una transformación notable. Comencemos por aclarar que, *medio de pago* es todo aquello que tenga un poder liberatorio de las obligaciones, como el dinero, la permuta, las prestaciones de hacer o no hacer, los efectos de comercio, etc. etc. En nuestro Código Civil el pago es, genéricamente, todo cumplimiento de una obligación debida, el *solvere* o liberación de la carga (art. 1.157 C.C.). Los medios de pago admitidos se detallan en el art. 1.156 C.C. (hacer, no hacer, permuta, compensación y entrega, y dentro de estas últimas, la entrega de dinero). Sin embargo, en sentido más popular, pago se identifica con el cumplimiento de las obligaciones pecuniarias en dinero en las que cambiamos capital real (bienes o servicios) por capital monetario (dinero o signo que lo represente). Aquí es donde la doctrina distingue entre el pago líquido o en moneda de curso legal y el pago que para el C.C. son fórmulas de dación en pago mediante medios de pago o signos representativos del dinero.

Por el contrario, *instrumento de pago* es el vehículo empleado para hacer efectivo el medio de pago, y por tanto hablamos de monedas, cheques, letras de cambio, transferencias, giros etc. Si a un instrumento de pago le añadimos el adjetivo electrónico estaremos indicando que para la satisfacción de la obligación se utilizan instrumentos o sistemas electrónicos para transferir a distancia el valor entre las partes acreedora y deudora.

Nos movemos pues en el difuso campo de los instrumentos de pago a distancia por medios electrónicos, entre los que estarán por un lado aquellos que poseen una regulación legal como los instrumentos bancarios de pago a distancia (instrumentos que permiten a su titular acceder a fondos depositados en entidades de crédito por lo que se autorizan pagos a un beneficiario: transferencias, retiradas de efectivo en cajero, pagos con cargas en dispositivos, pagos con tarjetas, etc.), los instrumentos de dinero electrónico (o instrumento de pago recargable, distinto de un instrumento de pago a distancia, en el que se carga en una tarjeta o una memoria de ordenador en el que se almacenan electrónicamente los valores en divisa en formato electrónico que permiten a su titular efectuar transacciones como la transferencia de fondos, el pago en entidades distintas del emisor o el reintegro de los valores) y finalmente, los instrumentos de pago no regulados o sin reconocimiento legal directo, como el cambio de valor en criptomonedas, que es el que ahora nos interesa.

Así pues, para realizar un contrato autoejecutable necesitamos un instrumento de pago electrónico, pero no nos valdrá uno cualquiera, en la medida en que requieran de la autorización de pago, la realización de pruebas de identidad u otros factores que excluyan el automatismo. Ciertamente nada hace imposible pactar una transferencia electrónica que opere con respuesta automática liberando fondos ante una señal convenida, mecanismo conocido en la banca p. ej. en los créditos documentarios de entrega garantizada contra documentos, pero factores como la aceptación de la orden de pago, el protocolo de identificación del cliente, la comprobación de fondos, la posible retirada de los mismos, la denegación de las transferencias o pagos por tarjeta en los que el cliente no introduce su clave o firma, los plazos de ejecución bancaria y de verificación, etc. etc. hacen que no haya oferta comercial financiera articulada para este modelo de contratación, y que se pueda abrir la puerta a vías de bloqueo a la ejecución del contrato, que por definición, atentan contra el espíritu y finalidad del tipo contractual.

Sólo los mecanismos de entrega automatizados se adaptan a la finalidad del negocio y aquí están principalmente, los instrumentos de dinero electrónico o la entrega/trasferencia de valor por medios electrónicos articulada en **criptomonedas virtuales**, entendiéndose por tales a las representaciones digitales de valor que pueden ser intercambiadas por medios telemáticos y que sirven como instrumento de cambio y/o unidad de valor o almacenamiento de valor, pero que no tienen un estatus legal de respaldo como divisa, pues no están garantizadas por ninguna jurisdicción, por lo que cumple con las citadas funciones solo por el acuerdo de la comunidad de usuarios en la que se utiliza⁹.

Personalmente he tenido ocasión de defender anteriormente¹⁰ que a mi juicio el mecanismo más idóneo para la concertación y ejecución de Smart contracts es el dinero electrónico, por su funcionalidad como instrumento de pago electrónico, su respaldo legal, su reconocimiento como divisa dotada de convertibilidad¹¹, y su estabilidad en el cambio frente a la volatilidad de las criptodivisas, que con frecuencia la hacen inútiles para articular un sistema de contratación marco estable y destinado a durar en el tiempo. El dinero electrónico, además, en tanto es dinero con reconocimiento legal, aunque no es de aceptación obligada ex art. 1.166 C.C., por no ser entrega en numerario para nuestro Código Civil, posee efectos solutorios reconocidos por el art. 1170.1 C.C. (entrega de efecto pro

9. Siguiendo a la Financial Action Task Force (FATF), Virtual Currencies – Key Definitions and Potential AML/CFT RISKS, 2014.

10. ECHEBARRÍA SÁENZ, M. «Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología Blockchain» en *REE*, monográfico, economía colaborativa, 2, 2017, ISSN: 2530-9854, págs. 65-93. Págs. 72 y ss.

11. Directiva 2009/110/CE, 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 (LA LEY 10372/2005) y 2006/48/CE y se deroga la Directiva 2000/46/CE. ley 21/2011 de 26 de julio de dinero electrónico, BOE 27 julio 2011, que sustituye al régimen de Ley 44/2002, de 22 de noviembre, de medidas de reforma del sistema financiero y el Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico, que lo desarrollaba.

solutivo)¹² sin depender del concepto de «buen fin» del art. 1170.2 C.C. (entrega de efectos «pro solvendo»)¹³.

A mayores, al dinero electrónico le es aplicable la normativa tutelar de la ley 16/2009 de 13 de noviembre de servicios de pago¹⁴, y la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior (DSP2)¹⁵, que unifican los derechos de los usuarios de servicios de pago en el SEPA (Single Euro Payment Area) e incluso puede aplicarse a pagos en los que uno de los operadores reside fuera del espacio económico europeo, todo ello bajo la supervisión del Banco Central Europeo y de los Bancos Centrales Nacionales. Las entidades de dinero electrónico y las de servicios de pagos quedan sometidas a una regulación similar a la bancaria y bajo la supervisión, en nuestro caso, del Banco de España. La ley de servicios de pago establece un estatuto de derechos de los usuarios, *irrenunciable* (plazos de ejecución, información precontractual, limitaciones en las condiciones de cobro por servicio, etc.) que beneficia a las partes por su aporte de seguridad jurídica.

Además, finalmente, la paulatina reducción de la admisión de pagos en numérico derivada de las leyes de contratación con la administración pública y de la normativa de prevención de blanqueo de capitales, nos lleva de manera inexorable a que determinados pagos deban ser hecho mediante anotaciones de dinero bancario o de dinero electrónico¹⁶. Cada vez con más frecuencia, la utilización del instrumento de pago bancario o de dinero electrónico se suma a los requisitos de validez o admisibilidad del contrato subyacente.

12. Cuando en la directiva 2000/46, se indicó que un euro digital equivalía a un euro en moneda-divisa con equivalencia-paridad y convertibilidad, se nos dijo que el pago en dinero electrónico equivalía al pago en euros nominales ordinarios, y por tanto, que también era un pago con *efecto solutorio inmediato o pro soluto* (art. 1170.1 C.C.), pero no impuso que fuera dinero de curso legal, puesto que es un instrumento electrónico de pago.
13. Con mayor extensión, ECHEBARRÍA SÁENZ, J.A., «El dinero electrónico: construcción del régimen jurídico emisor-porteador» en MATA MARTÍN, R./JAVATO MARTÍN A. *Los medios electrónicos de pago*, Granada Comáres, 2007, págs. 219-267. Ídem en ECHEBARRÍA SÁENZ, M. «Contratos electrónicos autoejecutables...», en *REE*, 2017, Págs. 72 y ss.
14. Que tiene su origen en la derogada Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior por la que se modifican las Directivas 97/7/CE, 2005/65/CE y 2006/48/CE. También interesa Reglamento (CE) n.º 924/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativo a los pagos transfronterizos en la Comunidad y el Libro Verde de la Comisión, de 11 de enero de 2012, titulado «Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por internet o pagos móviles».
15. y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.
16. la normativa sobre control fiscal y blanqueo de capitales restringe el pago en nominal a 3000 € y el uso de billetes de 500 €, obligando a que la mayor parte de las transacciones mercantiles se hagan por instrumentos de pago con apoyo en Cuentas Corrientes bancarias o por medio de instrumentos de dinero electrónico que gozan de reconocimiento legal. Véase principalmente RD 304/2014 de 5 de mayo en desarrollo de la ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y la financiación del terrorismo. <http://www.seplac.es/espanol/legislacion/norma-blanqueo.htm>

¿Qué es lo que explica entonces que la inmensa mayoría de las plataformas de contratación automática no usen la moneda digital de curso «legal» (o más bien reconocido como instrumento de pago) y en su lugar prefieran el uso de criptomonedas de emisión privada (bitcoins, ethers, y otras de las 1200 criptodivisas existentes), sin reconocimiento legal, frecuentemente inestables por su función especulativa¹⁷, y sin supervisión ni garantía de solvencia de la autoridad financiera? A mi juicio el principal motivo reside en la escasez de oferta comercial. El sector de la emisión de dinero electrónico está fuertemente bancarizado y las entidades de crédito no terminan de lanzar y promover este instrumento de pago en la dimensión que su potencial aporta. A día de hoy, cuesta articular un sistema de pago automatizado en euros digitales, porque las entidades de pago, mayormente entidades de crédito, siguen dando prioridad a los instrumentos de pago a distancia que implican la necesaria posesión de una cuenta corriente y el pago de comisiones por transferencia o tarjeta, que les resultan enormemente lucrativas. Mientras tanto, las criptomonedas de emisión privada han ido ocupando el hueco que el sistema legal no ha querido o no ha sabido llenar.

1. LA APARICIÓN DE LAS CRIPTOMONEDAS VIRTUALES CON TECNOLOGÍA BLOCKCHAIN; EL EJEMPLO DEL BITCOIN

Conviene aclarar que el intento de crear monedas virtuales se remonta a los años noventa del siglo XX. Diversos emisores intentaron crear divisas virtuales (mondex, liberty reserve dollars, e-gold, second life linden dollars, webMoney) con resultados diversos, pero mayormente fallidos¹⁸. La mayor parte de las monedas virtuales creadas en estos años fracasaron por cuestiones técnicas (riesgo de doble pago), sistémicas (estabilidad del sistema ante incrementos exponenciales de uso que requerían fondos de estabilidad y mecanismos de contención inexistentes), especulativas (falta de estabilidad en el cambio) o institucionales (los emisores carecían de recursos para poder actuar como un regulador-emisor monetario o bien fueron finalmente clasificadas como un sistema ilícito de blanqueo de capitales)¹⁹.

La mayor parte de estos factores, sin embargo, fueron superados con la aparición de la tecnología Blockchain.

Y considero necesario realizar una primera distinción. La llamada tecnología de bloques se basa inicialmente en la creación de un registro compartido y descentralizado, pero, en realidad, la tecnología de bloques puede usarse propiamente para crear sistemas plenamente descentralizados, sin una autoridad central o unidad rectora de las anotaciones que se incluyen en el registro compartido, **sistemas**

17. AA.VV., Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, «Price Fluctuation and the use of Bitcoin», en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.

18. MATEO HERNANDEZ, J. L., *El dinero electrónico en Internet Aspectos técnicos y jurídicos*. Granada, Comares, 2005. FATF. Guidance for a risk-based approach, *Virtual Currencies*, 2015.

19. FATF. Guidance for a risk-based approach, *Virtual Currencies*, 2015. MATEO HERNANDEZ, J. L., *El dinero electrónico... cit.*

disruptivos o descentralizados (Distributed Autonomus Organization: DAO) o bien pueden utilizarse como una simple herramienta contable bajo el control y dirección de uno o varios nodos responsables, es decir, utilizar el sistema contable compartido (*Distributive Ledger*), pero no la estructura descentralizada (**sistemas permisionados, dirigidos o managerizados (GSD-DTL)**). Propiamente, los sistemas de criptomonedas al uso y significativamente Bitcoin, son sistemas DAO, pero la tecnología de contabilidad distributiva se está expandiendo rápidamente a diversas aplicaciones empresariales bajo el control de managers del sistema (DTL).

La base tecnológica de los Blockchain reside en la combinación de los sistemas de comunicación Peer to Peer (puerto a puerto) con los sistemas de firma o acreditación por mutua confianza que aparecen con el sistema PGP (*Pretty Good Privacy*) en los años noventa²⁰. La propuesta de usar un sistema de acreditación mutua basada en el consenso y en la computación criptológica para crear un instrumento de pago no oficial se atribuye a Satoshi Nakamoto (que es un pseudónimo) en 2009²¹. La propuesta de Nakamoto fue polémica y generó tanto entusiasmo en la red como rechazo en el sistema financiero²². Sin embargo, al paso del tiempo el sistema ha demostrado ser viable y sobre todo, computacionalmente resistente.

Bitcoin propiamente es un protocolo o programa descargable en cualquier ordenador que crea una plataforma de nodos y usuarios descentralizada y sin intermediarios ni autoridad de supervisión, para la conclusión y gestión de transacciones de cambio (Bitcoins), creando un ecosistema digital. El objetivo del protocolo Bitcoin es la transmisión de Bitcoins; «moneda digital» creada por el propio sistema, al que se atribuye valor de cambio por la aceptación de terceros que se afilian al sistema contable Bitcoin. El sistema contable Bitcoin resultó ser rápido y computacionalmente confiable desde el momento en que no ha habido un número de errores de sistema que lo hayan puesto en riesgo, o al menos no lo bastante como para provocar la huida del sistema. En la actualidad Bitcoin supera los noventa mil millones de dólares en valor y crece diariamente²³: Bitcoin, sin embargo, ha resultado ser no sólo un medio de pago electrónico automatizable, sino también un instrumento de inversión especulativa²⁴, un instrumento de evasión fiscal, blanqueo

20. Creado por Phil Zimmerman en 1991 utilizando los sistemas de criptografía asimétrica o de clave pública. Véase https://es.wikipedia.org/wiki/Pretty_Good_Privacy.

21. Nakamoto Satoshi, (pseudónimo), Bitcoin: «A Peer-to-peer Electronic Cash System», 2008, <https://bitcoin.org/bitcoin.pdf>

22. European Central Bank, Virtual Currency Schemes, Report, october 2012, in www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (e informes posteriores año por año). febbraio 2015, in www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf;

Banco central Europeo: Opinion on virtual currencies, Report, 4.7.2014, in www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf así como advertencias de prácticamente todos los bancos centrales europeos. Un resumen de posiciones en informe FATF. *Guidance for a risk-based approach, Virtual Currencies*, 2015.

23. <https://blockchain.info/en/charts/market-cap>

24. Instrumento especulativo altamente volátil según los estudios: Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, «Price Fluctuation and the use of Bitcoin», en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.

de dinero y facilitación de operaciones en negro²⁵, lo que aumenta su carácter polémico exponencialmente. Sin embargo, para hacer un juicio ecuánime del sistema es necesario analizar con más profundidad su funcionamiento, sus virtudes y sus riesgos.

2. LA TECNOLOGÍA DE LA CADENA DE BLOQUES: FUNCIONAMIENTO DE LOS REGISTROS COMPARTIDOS O DISTRIBUTIVE LEDGER

Desde la aparición del dinero contable o dinero bancario²⁶, todo sistema de contabilidad se ha orientado a impedir el doble cómputo o doble pago de una anotación. En una transacción ordinaria el dinero físico sólo existe en una ubicación, o en nuestro bolsillo o en el del vendedor. Ni podemos gastar el mismo billete dos veces ni podemos tenerlo en dos sitios. Los bancos en sus sistemas contables emulan este mismo comportamiento, las retiradas de dinero se emulan contablemente mediante un sistema de anotación-desanotación contable en debe y haber. La compensación automática previene del doble gasto o del doble apunte²⁷.

La actividad de control frente al doble pago es relativamente fácil cuando hay una autoridad central supervisora del sistema y es responsable de la emisión de la moneda contable, es decir, un sistema público de respaldo que cumple con las funciones de supervisión y garantía del sistema. La novedad, y dificultad que presenta bitcoin y los sistemas similares, es la de que no existe dicho intermediario-supervisor: son los propios usuarios del sistema los que supervisan y admiten las operaciones, cada operación, a través de un sistema difuso de acreditación mutua. El control es posible gracias a la existencia de una base de datos única, de construcción colectiva, compartida por todos los nodos (o «mineros»)²⁸ que utilizan el sistema. Así, los usuarios autorizados introducen cada operación usando un protocolo común y respetando una línea temporal de marcado que evita la retroactividad y exige la coherencia de cada operación con las anteriores. El protocolo busca acreditar la certeza de la operación, su unidad y su inmutabilidad mediante una «prueba de trabajo» computacional que consiste en la resolución de complejos algoritmos y que debe ser confirmada a su vez por otros operadores del sistema. Las operaciones confirmadas por el sistema se integran en un bloque de computación que son base de las siguientes y van quedando sepultadas por las posteriores en una cadena interminable de operaciones superpuestas (cadena de bloques o blockchain). El resultado es tal que, alterar la base de datos retroactivamente, exigiría

25. FATF. *Guidance for a risk-based approach, Virtual Currencies*, 2015

26. BONET CORREA, J. *Las deudas de dinero ...* Cit.

27. <https://www.oroyfinanzas.com/2013/10/bitcoin-block-chain/>

28. Se llama mineros al individuo o entidad que participa en una red descentralizada de divisas virtuales utilizando un software especial para resolver complicados algoritmos en una prueba de trabajo distribuida o sistema distribuido de prueba/verificación usado para validar las transacciones y anotaciones contables del sistema de moneda virtual. FATF *Virtual Currencies key definitions ...* 2014.

una capacidad computacional casi imposible de obtener hoy por hoy, pues, supone la necesidad de superar como mínimo el 51% del poder computacional de todos los miembros del sistema. El conjunto genera así una estructura de control, sin gobierno, que minimiza el riesgo de manipulación por uno o varios usuarios, pues las modificaciones exigen una operación idéntica de sentido contrario que exigiría el consentimiento de todos los partícipes. La totalidad de la red puede supervisar y comprobar el sistema y controlar la coherencia contable de la cadena, por lo que no cabe una intervención directa que altere sus términos.

El sistema se basa pues en la mutua acreditación de confianza. Es el consenso mayoritario de los usuarios el que acredita la legitimidad de una operación y la última versión del **registro blockchain**. Registro blockchain en el que los sucesivos bloques de computación que se añaden por los «mineros» de datos (nodos) a la cadena, se refresca cada 10 minutos gratuitamente y sin interrupción. Así, cualquier elemento del sistema puede introducir un dato-transacción en el mismo, pero la existencia y veracidad de la transacción no está aún verificada. La veracidad de la operación en un sistema descentralizado se constata cuando la transacción se inserta en un blockchain y luego se crean nuevos bloques sobre este, que van confirmando la transacción que hemos realizado. Una operación no es refrendada hasta que al menos seis nodos o mineros la refrendan. Al conseguir ser verificado por más elementos del sistema e incorporarse a la cadena la estructura del sistema asume como «verdaderos» aquellos bloques de la cadena más larga que tengan 5 o más bloques encima del mismo. Un bloque que se haya extendido con 5 bloques más muestra un total de seis confirmaciones como mínimo. Una bolsa de cambio de valor, como es Bitcoin, no se puede exponer al riesgo del doble gasto. Por eso solo puede transferir los Bitcoins a la cuenta de un cliente cuando se haya confirmado como «verdadera» y, es precisamente por eso, que ignorará los bloques hasta que no sean parte de la cadena más larga y no tengan más de seis confirmaciones. Una copia completa de la Blockchain (registro Blockchain) contiene todas las transacciones ejecutadas en la divisa y con esa información uno puede saber qué valor ha sido propiedad de cualquier dirección, en cualquier momento desde la existencia de la base de datos²⁹. Bitcoin, pues, se basa en la trazabilidad de la divisa electrónica desde su origen para asegurar su valor. Cada bloque tiene un hash o huella electrónica desde el génesis hasta la actualidad y permite un orden cronológico que impide el doble pago (tendrías que modificar todos los bloques anteriores). El sistema prima la generación honesta en la que la cadena más larga, por su dificultad combinada³⁰, y por su mayor respaldo computacional, es más fiable. Una cadena es válida si todos sus bloques previos son confiables y permiten el acceso hasta el génesis. Para cualquier bloque de la cadena solo hay un camino al génesis block.

Este sistema de refrendo colectivo resulta ser sorprendentemente fiable, pero aquí hay que señalar un riesgo del sistema: En un momento dado puede haber dos o más bloques al mismo nivel, con contenido contradictorio y compitiendo por

29. <https://www.youtube.com/watch?v=8zgvzmKZ5vo>

30. <https://www.youtube.com/watch?v=9V1bipPkCTU>

procesar la misma transacción y convertirse en el próximo bloque de la Blockchain, son los llamados **forks** bifurcaciones u horquillas³¹ que se crean cuando dos bloques son creados con solo unos pocos segundos de diferencia. Este fenómeno no debe confundirse con el de la aparición de plataformas falsas (Scrum) que simulan la computación de Bitcoins para recabar inversiones fraudulentamente³². En este caso nos referimos a la aparición de una horquilla que pone un valor Bitcoin en conflicto entre dos potenciales titulares. Cuando pasa eso, los nodos siguen construyendo la cadena sobre el bloque que hayan recibido primero. Los bloques de cadenas más cortas no serán validadas y finalmente serán desestimadas: todas las transacciones que forman parte de la cadena corta se reagrupan en las transacciones pendientes y se incluyen en otro bloque. La recompensa para los bloques en la cadena más corta no estarán en la cadena más larga, por lo que estarán perdidos en una lista RPCCall³³.

Esta es la razón por la que la red obliga un «tiempo de maduración» de 100 bloques para la generación de los Bitcoins que remuneran la labor computacional de los «mineros». El tiempo de maduración de un bloque se aplica para los bloques nuevos generados por los mineros de Bitcoin como medida de seguridad para evitar el doble uso de Bitcoins: un nodo minero de datos no podrá gastar o pagar nada con sus Bitcoins generados, hasta que su bloque esté a 101 bloques del bloque de más reciente creación.

Para aquellos supuestos en los que surge disputa sobre la titularidad del valor o la validez de una transacción, sin embargo, se ha creado un sistema de resolución de conflicto que resulta igualmente eficaz y coherente con el sistema. En la última versión del protocolo se introdujo el sistema multifirma (*multi signature*), que sustituye al primitivo sistema de resolución de conflictos por vía judicial o por un árbitro externo al sistema³⁴. Así, si aparece un conflicto sobre un fondo (titularidad de un bitcoin) con el sistema multi-sig, este quedará bloqueado en manos de un tercero que hará las funciones de árbitro en caso de controversia. La operación finalmente aprobada puede quedar con ello subordinada a la acreditación de la misma por un número pre establecido de sujetos interesados/involucrados. El sistema, en definitiva, otorga en caso de controversia sobre la titularidad de un Bitcoin entre A y B, a quien C o más acreedores apoyen como parte vencedora del litigio, sin que

31. <https://www.youtube.com/watch?v=Lx9zgZCMqXE>

32. Como ejemplo local la moneda virtual unite de Unetenet que resultó ser un fraude de más de 50 millones. véase www.bolsamania.com/noticias/tecnologia/que-es-el-unete-una-estafa-de-50-millones-de-euros-a-partir-del-bitcoin-de-jose-manuel-ramirez--771685.html
www.noticiasespanolas.es/index.php/483471/prision-para-los-dos-fundadores-de-unete-la-estafa-de-la-monedavirtual-espana/
www.lasexta.com/noticias/sociedad/detienen-responsables-estafa-piramidal-unetenet-2015102657245f4d6584a81fd882a0f7.html

33. https://en.bitcoin.it/wiki/API_reference_%28JSON-RPC%29

34. Oermann-Töllner, The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration, https://cyber.harvard.edu/publications/2014/internet_governance_in_bitcoin

ninguna de las partes, árbitro/s incluidos, puedan disponer del fondo hasta que se produzca dicho consenso.

Y dicho esto, el sistema arbitral puede dirimir la cuestión de la titularidad sobre un Bitcoin, o sobre la legitimidad de una cadena, si se prefiere así, pero eso no impide que los titulares de la cadena más corta, la desestimada, puedan ver defraudados sus intereses, planteando un problema de responsabilidad.

Por completar la visión del sistema: para solucionar los posibles problemas de obsolescencia y asegurar la evolución del sistema la evolución del software y la supervisión técnica del sistema se encomienda a una fundación, sin ánimo de lucro, la **Bitcoin Foundation**³⁵. La importancia de esta fundación en la adaptación e innovación del sistema es esencial, pero en modo alguno es un órgano rector o un supervisor del sistema como tal.

3. SECRETO Y CRIPTOGRAFÍA DE SEGURIDAD EN BITCOIN

Conforme a lo expuesto, todo el mundo puede comprobar la cadena de bloques y ver el momento y circunstancias de una transacción. Esta transparencia permite el contraste con los datos aportados por los usuarios, pero el sistema permite el seudónimo y por ello no identifica necesariamente al usuario de cada transacción. Comprobar una operación no es lo mismo que comprobar la autoría de la misma. Blockchain no exige la identificación previa de un usuario, lo identifica por una serie de códigos/claves y una copia criptográfica con un sistema de criptografía publica de doble clave, por lo que cada usuario tiene sus claves almacenadas en un portafolio independiente que debe controlar, pues el único medio de identificación de la titularidad de la operación, con el inconveniente de que la apropiación o la pérdida de las claves harían imposible acceder al Bitcoin. Es cierto que se pueden usar mecanismos de identificación indirectos; IP del proveedor de servicios, adjuntado de correos, vinculación de la operación a CC bancaria... por lo que el sistema se califica como pseudo secreto, pero el sistema en si permite y facilita el anonimato del titular, y la combinación del sistema con mecanismos como los de navegación anónima, uso de la red TOR³⁶ y similares, pueden hacer imposible la identificación del titular, motivo por el cual se ha convertido en una panacea para quienes buscan su uso en transacciones ilícitas o en el blanqueo de capitales.

4. ANÁLISIS DE RIESGOS PARTICULARES Y SISTÉMICOS DEL BITCOIN

De hecho y abundando en lo ya indicado, Bitcoin presenta diversos riesgos particulares y algunos riesgos sistémicos que conviene exponer para valorar el sistema.

35. <https://bitcoinfoundation.org/>

36. www.torproject.org

4.1. Riesgos individuales en Bitcoin

Entre los riesgos particulares está el de que alguien se haga con nuestra clave privada para usar el sistema de criptografía de clave pública: por ejemplo, asaltan nuestra wallet, copian el archivo «wallet.dat». Si usamos clave personal estas son bastante accesibles frente a asaltos de computación basados en el diccionario las palabras de uso frecuente o de claves numéricas vinculadas al usuario. Un programa de ataque normal usa cuatro millones de palabras básicas de las que destacan unos pocos miles y en el que se afina con más rapidez introduciendo datos básicos del usuario³⁷. Por otro lado, si no dispones de copia y te olvidas o pierdes la clave, pierdes para siempre el acceso al Bitcoin, que queda perdido en el ciber espacio. Se calcula que una cantidad superior a los 22 millones de euros navega por el ciber espacio en esta condición de limbo³⁸.

¿En qué cartera de almacenamiento confiar? ¿En una depositada en la nube (Hotwallet)?, ¿en tu ordenador o en dispositivos de almacenamiento? (coldwallet)³⁹ La utilización de plataformas de intercambio interpuestas añade, además, un factor de riesgo, ya que algunas son muy vulnerables.

El segundo riesgo de seguridad personal deriva de la propia dinámica de funcionamiento: si se te estafa para realizar un pago, no hay vuelta atrás, la cadena es irreversible y los nodos no responden de la introducción de los datos en el bloque, por lo que sólo cabría una compensación por quien nos ha estafado como forma de reversión, lo que por definición es improbable. En sentido parecido, si alguien nos «coloca» en una cadena insegura, en un *fork* destinado a fracasar, descubriremos que, en propiedad, nadie dentro del sistema responde por ello.

4.2. Riesgos sistémicos de Bitcoin

Pero lo que en realidad debe preocuparnos más, es si el propio sistema presenta riesgos que lo hagan inhábil para los fines funcionales que aquí se pretenden.

Bitcoin parece un sistema resistente frente al **riesgo tecnológico**. El sistema de hoja contable compartida o base de registro única compartida que se crea es computacionalmente resistente. Un ataque computacional contra la cadena implicaría utilizar una capacidad de computación que supere al menos al 51% del sistema distribuido, lo que es harto difícil y aún más teniendo en cuenta la existencia de registros previos y la descentralización del sistema. Con excepción de un incidente en el momento incipiente del nacimiento de la cadena, que no quedó nunca bien aclarado, el sistema ha resultado ser confiable. Ello no obstante, no es impensable un riesgo de colapso derivado de la propia dinámica del sistema, que no admite más de tres transacciones por segundo, lo que puede ser insuficiente ante el crecimiento

37. http://www.eldiario.es/hojaderouter/seguridad/seguridad-carteras-bitcoin-hackers-criptomonedas_0_363264145.html

38. www.bitcoinfoundation.org

39. <http://www.technologyreview.es/informatica/44368/escribe-la-clave-de-tus-bitcoins-en-un-papel-si/>

exponencial del uso de la red⁴⁰. Peor es la respuesta frente al **riesgo sistémico**: ni los nodos o mineros de Bitcoin ni los diversos agentes intermediarios e inversores que operan en el sistema se someten en realidad a norma de garantía alguna, ni responden de la introducción de datos en el sistema. Diversas compañías especulativas en Bitcoin han quebrado, y esto causa trastornos y pérdidas a los usuarios, pero lo más inquietante es lo que esto supone por cuanto indica que no hay mecanismos de contención frente a un hundimiento generalizado de los agentes. Bitcoin protagoniza constantemente fluctuaciones de su cotización que mayormente se resuelven al alza⁴¹, pero un abandono repentino y generalizado del sistema hundiría su cotización y podría provocar un crack del sistema en su conjunto, sin que hubiera mecanismos de control como los existentes en el sistema target, el sistema de pago interbancario o en cualquier otro sistema de compensación financiera supervisado. En los sistemas de compensación de pagos europeos se establecen mecanismos de control de concentración de riesgo, de paralización temporal de operaciones ante caídas repentinas o acumulaciones inusuales de movimientos de caja, que actúan como colchón del sistema y que podrían haber protegido a múltiples usuarios ante el hackeo de operadores en bitcoin o ante quiebras de dichos operadores. De hecho, uno de los mayores riesgos de Bitcoin es el **riesgo institucional**; que sean las propias autoridades bancarias las que coordinen un ataque en forma de prohibición de operación, como la decretada por la autoridad bancaria China, pues si finalmente las criptomonedas virtuales tiene problemas para su conversión en divisa ordinaria o para realizar operaciones de pago, los usuarios forzarían la desinversión masiva y esto podría provocar el colapso del sistema⁴². Sorprendentemente, sin embargo, es necesario aclarar que aunque la prohibición de China supuso bajadas de un 16 a un 22% en las criptodivisas, éstas se recuperaron en menos de una semana y han continuado subiendo en la cotización.

Hay, por otro lado, una lección a aprender del **riesgo mutualista o de coherencia** evidenciado por los llamados «**hard forks**»⁴³ o con más propiedad, de la

40. Una de las razones alegadas para la producción del hard fork (vid infra) fue el cuasi colapso del sistema en 2016 cuando las transacciones llegaron a completarse en plazos de 43 minutos y se llegó a rechazar operaciones por bloqueo del sistema. www.gurusblog.com/archives/bitcoin-al-borde-del-colapso-tecnico/06/03/2016/
41. Polasik-Piotrowska-Wisniewski-Kotkowski-Lightfoot, «Price Fluctuation and the use of Bitcoin», en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.
42. https://cincodias.elpais.com/cincodias/2017/09/04/mercados/1504518523_957352.html
http://www.abc.es/economia/abci-prohibicion-china-pone-fiesta-monedas-digitales-201709100129_noticia.html
<https://urbantecno.com/tecnologia/bitcoin-ethereum-china>
43. <https://elbitcoin.org/escenarios-posibles-partir-del-fork/>
<https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#a742865337d4>
<https://www.xataka.com/empresas-y-economia/mas-forks-de-bitcoin-mas-incertidumbre-a-bitcoin-cash-se-le-suman-bitcoin-gold-y-el-seguit2x>
<https://criptotendencia.com/2017/09/29/primero-cash-ahora-gold-otro-hard-fork-de-bitcoin-esta-en-camino/>
<https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-que-C3%A9-consisten-y-cu%C3%A1les-sus-diferencias>
<https://www.coindesk.com/bitcoin-cash-developers-set-date-november-hard-fork/>

división del sistema que se produce cuando es la comunidad de mineros la que se divide y duplica la cadena entera, creando dos líneas separadas de desarrollo por modificación del protocolo asumido, como cuando Bitcoin se separó en Bitcoin cash y Bitcoin gold.

Al dividirse la cadena de nodos en el uso de dos protocolos, ambos tomando la cadena de bloques original como base, lo que ocurre es que los titulares de posiciones en la cadena vieron duplicadas sus anotaciones, aunque eso sí, la división afectó a la valoración de ambos nominales devaluando (inicialmente) la cotización previa. Esta multiplicación es, desde el punto de vista contable inadmisibles y aunque el sistema obviamente resistió la operación, dio lugar a movimientos especulativos con los nuevos y los viejos nominales⁴⁴ y demostró que un sistema basado en el consenso estructural puede morir si dicho consenso estructural se pierde, pues realmente nadie dirimió la titularidad de la cadena y un sistema monetario no puede duplicar sus activos, sin base real, indefinidamente. Detrás de una divisa o de un valor de cambio, necesariamente ha de existir una base de capital real (PIB de las naciones, bienes) o de capital Monetario (divisas). Un sistema que duplica el valor residente, aunque sea nominalmente, carece de estabilidad y credibilidad a largo plazo. Al menos como moneda, otra cosa es, ciertamente, como valor especulativo. Tras la división de la cadena Bitcoin, de hecho su cotización se ha revalorizado a niveles nunca vistos, en lo que reproduce un sistema de hiperinflación virtual altamente arriesgado, Pero esto implica que, juegos de inversión aparte, las criptomonedas o introducen sistemas de control del riesgo sistémico o terminarán por no ser instrumentos aptos para la contratación regular y masiva del Business to Business, pues nadie puede un articular un sistema de intercambios regular sobre una divisa hiperinflacionaria o hiperdeflacionaria en el que se desconoce finalmente cuál es el valor comprometido en la transacción. Bitcoin, por desgracia, se ha convertido más en un valor que en una moneda. No es de extrañar que el Banco de España considere la transacciones en bitcoins como más cercanas a una operación OTC en un mercado descentralizado que al mercado monetario⁴⁵.

IV. RÉGIMEN JURÍDICO DE LAS OPERACIONES EN CRIPTOMONEDAS VIRTUALES

La tecnología Blockchain ha sido identificada como tecnología disruptiva⁴⁶ en contraposición a la llamada tecnología de sustentación al crear sistemas horizontales y descentralizados sin una autoridad rectora o supervisora, momento en el que aparece un riesgo de gobernabilidad y de definición del estatus jurídicos

44. CHERNUKKA, V., «Como influencia el hard fork al precio del bitcoin» <https://blog.iqoption.com/como-influencia-el-hard-fork-al-precio-del-bitcoin/> 30-10-2017
45. GORJÓN, S., Banco de España, Eurosistema, Dirección General de Operaciones, Mercados y Sistemas de Pago, «Divisas o Monedas Virtual: El caso de Bitcoin» ENERO 2014, PÁG. 4/13.
46. Bower-Christensen, «Disrupting Technologies: Catching the Wave», in *Harvard Business Review*, I, 1995, 43. SWARTZ, LANA, «El sueño del Blockchain. Imaginando alternativas tecnoeconómicas más allá del bitcoin» en CASTELLS, M. et al. *Otra economía es posible. Cultura y economía en tiempos de crisis*. Alianza editorial, Madrid, 2017, págs. 123-155

(ley y foro aplicable)⁴⁷, así como una clara dificultad para identificar a los sujetos responsables. El estatus jurídico de los operadores en Bitcoin es, a día de hoy, ciertamente confuso.

1. HACIENDA PÚBLICA

Sabemos, por diversas consultas vinculantes a la Hacienda Pública (V3625-16, V 1028-15, 1029-15, V2846-15) que los mineros de Bitcoin están obligados a darse de alta en Hacienda (*licencia de actividad económica*) y a pagar en su caso la cuota de autónomos por desarrollar una actividad económica. Minar, se tenga beneficios o no, es una actividad económica y el titular de la actividad está obligado a darse de alta en el Impuesto de Actividades Económicas como «Otros servicios financieros no comprendidos en otras partes»⁴⁸. El minero individual debería darse de alta en la Seguridad Social, incluso si no llegara a generar bloques, y debería reflejar los incrementos patrimoniales por sus ventas de Bitcoins en el IRPF o en el **Impuesto de Sociedades** según la forma jurídica empleada para el «minado».

Por el contrario, la actividad de minado en sí misma no está sujeta al IVA; la generación de la criptomoneda, para que fuera gravable por el impuesto, tendría que responder a una relación directa entre el servicio prestado y la contraprestación recibida, como señaló el TJUE (Sala Segunda) en su sentencia de 5 de febrero de 1981, asunto 154/80⁴⁹. La creación de bitcoins no presupone una relación entre el proveedor y el destinatario del servicio «de tal forma que en la actividad de minado no puede identificarse un destinatario o cliente efectivo de la misma, en la medida que los nuevos Bitcoins son automáticamente generados por la red»⁵⁰. Por ello, el minado de criptomonedas que genera nuevos bloques en la red no estará sujeto al IVA, pero, ¡cuidado! el cobro de comisiones que no aumenta la masa monetaria, si estaría sujeto a tributación del IVA. Y minar bitcoins, tampoco daría derecho a desgravarse las cuotas de IVA soportadas (art. 94 LIVA).

Del mismo modo, la primera transmisión de bitcoins estaría sujeta al IVA, pero sería una operación exenta⁵¹. Si no entiendo mal, ello implica que la no declaración de la primera transmisión de bitcoins, aun exenta, implica una sanción objetiva mínima de 300€.

47. Böhme-Christin-Edelman-Moore, «Bitcoin: Economics, Technology and Governance», in *Journal of Economic Perspectives*, Vol. 29, n. 2, 2015, 213.

48. Art. 78 TR LHRL epígrafe 831-9 de la sección primera de tarifas, «Otros servicios financieros no comprendidos en otras partes»

49. <https://www.abanlex.com/2016/09/los-mineros-de-bitcoins-estan-obligados-a-darse-de-alta-en-hacienda-y-pagar-la-cuota-de-autonomo/>

https://www.abanlex.com/wp-content/uploads/2016/09/V3625-16_anonimizada.pdf

50. V3625-16

51. V1029-15 y V2846-15 y TJUE en su Sentencia del asunto C-461/12 y asunto C-264/14 sobre la fiscalidad en el IVA de las transmisiones en bitcoins: https://www.abanlex.com/wp-content/uploads/2016/09/TJUE_C-264-14.pdf

Por otro lado y de manera incoherente con el tratamiento del IVA, para el ICAC, las monedas virtuales deberán calificarse como inmovilizados intangibles en la medida que cumplan con los requisitos expuestos en la NRV 5ª del PGC⁵².

Obviamente, la mayoría de los cientos de pequeños mineros no profesionales raramente cumplen con estos deberes. Obviamente también, Hacienda aún no ha encontrado la forma de detectar debidamente este tipo de transacciones dentro de su ámbito de competencia territorial, pero si llega a encontrar el método, el rosario de sanciones sería abrumador.

2. NORMATIVA DE PREVENCIÓN DEL BLANQUEO DE CAPITALS

Como es habitual en el campo tecnológico, fueron las autoridades de los EEUU las primeras en abordar esta cuestión cuando en marzo de 2013 el Financial Crimes Enforcement Network (FinCEN) del Departamento de Estado Norteamericano, extendió el alcance de la normativa BSA, tanto a las casas de cambio que efectuaban operaciones de compra/venta de las divisas virtuales por dinero de curso legal, como a quienes actuasen como «mineros» de Bitcoins, obligándoles a ambos a registrarse como empresas prestatarias de servicios monetarios y cumplir con la normativa de blanqueo de capitales y financiación del terrorismo, al considerar que en su actividad existía una transferencia de valor. No obstante, los usuarios que emplean Bitcoins exclusivamente como un medio de pago de bienes o servicios no se ven afectados por esta medida. La FINcen Norteamericana, de hecho, ya ha impuesto graves sanciones a operadores de Bitcoin por no cumplir con los planes de prevención del blanqueo de capitales⁵³.

La postura contrasta con la sostenida hasta el momento por el FATF europeo que, aunque considera que Bitcoins no pueden considerarse moneda corriente, dinero electrónico o instrumento financiero en el sentido ordinario, y por tanto no sujeta directamente estas operaciones a la normativa anti blanqueo (FATF informe 2014), sí que recomienda a las autoridades nacionales y europeas que utilicen los marcos legislativos actuales de regulación y supervisión para que sean aplicables a las monedas virtuales, y que, si no fuere posible, procedan a su modificación y adaptación (Informe 2015). El plan europeo de lucha contra el terrorismo (Com 2016 50 final) ya propone abiertamente la modificación de la directiva de prevención del blanqueo de capitales para incluir las agencias y plataformas de moneda digital en el ámbito de supervisión. En el caso de España, estas recomendaciones, pese a que no ha habido una reforma legal de inclusión, ya han sido aplicadas de hecho y de Derecho, con el respaldo que dio las SAP de Asturias de 6 de febrero de 2015 a la aplicación del art. 7.3 de la LPBC a los agentes de Bitcoin⁵⁴.

52. Contestación a Consulta del Instituto de Contabilidad y Auditoría de Cuentas (ICAC). Rfa: rnr/38-14.

53. Véase RAMOS SUÁREZ, F. (Presentación) LA REGULACIÓN JURÍDICA DE LAS MONEDAS VIRTUALES Y LA TECNOLOGÍA BLOCKCHAIN, Fide DPO it Law, mayo 2016 (Disponible en red)

54. Un comentario en <https://www.royfinanzas.com/2015/04/aplica-ley-prevencion-blanqueo-capitales-bitcoin-espana/>

3. NORMATIVA DE SERVICIOS DE PAGO

Determinar si las compañías que operan en Bitcoin u otras criptomonedas son compañías de servicios de pago es una labor más delicada. Acudiendo nuevamente al ejemplo norteamericano, en los USA los transmisores de Bitcoins se consideran transmisores de dinero y como tal deben obtener la correspondiente licencia estatal y someterse a la normativa de secreto bancario y de negocios de servicios en moneda virtual (*Virtual Currency Business Services*). Diversos estados como New York, Dakota o California han regulado licencias estatales para estas compañías de servicios monetarios virtuales, mientras que otros Estados se encuentran en proceso de aprobación de sus propias normas. Es aquí donde llamo la atención sobre el documento, *Uniform Regulation of Virtual Currency Businesses Act*, de Julio de 2017, elaborado por la National Conference of Commissioners on Uniform State Laws, por su especial valor, no sólo en la exposición del estado de la cuestión, sino también por los criterios de regulación y armonización que se propone a los Estados de la Unión. A juicio de los armonizadores de las legislaciones estatales, las licencias de servicios de monetarios se deberían limitar a aquellas compañías que realicen las funciones de: Control, Store, Trade, Exchange, Transfer. Es decir, control de los fondos monetarios, almacenamiento de los mismos o sus accesos, negociación de compra o venta de activos en criptodivisas, cambios de divisas y criptodivisas, y transferencias de fondos en criptodivisas. Y concretando aún más, se recomienda la exclusión de las operaciones *peer to peer* (entre particulares o entre particulares y empresas).

Mientras, en Europa, ni la directiva de dinero electrónico ni la directiva de servicios de pago es directamente aplicable al supuesto. Bitcoin no es una moneda en sentido técnico y por ello no estaría en el ámbito de dichas regulaciones⁵⁵, pero nuevamente se recomienda a las autoridades nacionales la aplicación del marco de supervisión en lo que sea admisible y la modificación del marco regulatorio en su caso a fin de someter a los mismos a un régimen de garantía. En concreto, los mineros de Bitcoin no son entidades de pago a los efectos de la LSP española, ni en los términos de la Directiva 2007/64 o en la más reciente Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago (DSP2). Tampoco pueden considerarse como las más recientes Entidades de Servicios de iniciación de pago⁵⁶.

Y dicho esto, sin embargo, lo que no es aplicable necesariamente a los mineros de Bitcoin o a los particulares que efectúan una operación de puerto a puerto, sí que se puede predicar de buena parte de los operadores de compra y venta de Bitcoins, que son perfectamente incluibles en las categorías legales, puesto que:

- Trafican Bitcoins con otras divisas; funciones Trade, Exchange
- Almacenan valores y claves (Hotwallets service)

55. Banco Central Europeo, Informe sobre monedas virtuales febrero 2015 y opinión de 4 de julio 2014.

56. ALVARADO HERRERA, L. «El servicio de iniciación de pagos en la Directiva 2015/2366 sobre servicios de pago en el mercado interior» en *La Ley mercantil* n.º 34, 2893, 2017.

– Transfieren fondos a cuentas de otros usuarios, bien directamente, en servicio de pago, bien como iniciadores de servicios de pago.

Conviene pues diferenciar entre el mercado primario o de emisión de Bitcoins y el mercado secundario o derivado de negociación de los mismos, que ocasionalmente si es susceptible de encuadramiento. Por otro lado, si bien no cabe definir a los mineros de Bitcoin como entidades de pago, las operaciones de pago en Bitcoin no están explícitamente excluidas del ámbito de la directiva DSP2 y las transacciones en Bitcoin organizadas por agentes de Bitcoins son encuadrables en la definición de operación de pago y sistema de pago de la DSP2 (art. 4 n.º 5 y 7). Del mismo modo, la función de Bitcoin como instrumento de pago es perfectamente coherente con la definición del art. 4.14 DSP2 por la que instrumento de pago es «cualquier dispositivo personalizado y/o conjunto de procedimientos acordados entre el usuario de servicios de pago y el proveedor de servicios de pago y utilizados para iniciar una orden de pago». A mi juicio, la futura trasposición de la directiva de servicios de pago 2015, previsiblemente establecerá algún mecanismo expreso de incorporación al régimen tutelar, no a los mineros de Bitcoin, que ciertamente no son incluibles en el tipo, pero si a las compañías que trafican con el cambio de divisas y Bitcoins o que actúan como pasarelas de pago o de iniciación de servicios de pago, admitiendo el pago en Bitcoins.

Esto supondrá una extensión de la seguridad jurídica de los usuarios del sistema, que podrán acogerse al régimen tutelar comunitario de los art 38 y ss. de la DSP2 (trasparencia informativa, gastos de información, carga de la prueba, información precontractual y condiciones generales, plazos de ejecución, etc.) pero también nos lleva al previsible contexto de diferenciación entre las compañías de pago en Bitcoins que regularicen su estatus jurídico y las que previsiblemente no lo harán o no estarán sujetas a dicha carga por no ser de ningún Estado comunitario. El panorama del uso del Bitcoin en los próximos años se prevé confuso porque, además, hemos de recordar que buena parte de la normativa cautelar choca frontalmente con el planteamiento de privacidad y anonimato de las redes Blockchain y en concreto del Bitcoin. Y sin embargo, en mi opinión, las criptomonedas están destinadas a incorporarse al sistema de pagos oficial y a poder funcionar normalmente como sistema de pago por más que previsiblemente queden reductos de operaciones opacas en la red. Lo mismo que ocurre a fin de cuentas con el dinero ordinario, que siempre ha tenido su mercado negro de transacciones no registradas.

4. NORMATIVA DEL MERCADO DE VALORES

Como se ha señalado anteriormente, Bitcoin y las principales criptomonedas, debido a su valor especulativo y su volátil cotización en el cambio, han terminado operando más como un signo de valor que como una moneda o instrumento de pago⁵⁷.

57. GORJÓN, S., «Divisas o Monedas Virtual...», 2014, Pág. 4/13.

¿Es quizás la aproximación a las criptomonedas como valor, la más apropiada?

Acudiendo nuevamente al ejemplo norteamericano la aplicación del *Howey Test* a las criptomonedas arroja un resultado parcialmente satisfactorio. Siguiendo el tradicional análisis para determinar si una oferta es una Security (o valor negociable) se dan los principales rasgos distintivos, puesto que, existe una oferta, se adquiere un bien jurídico inmaterial dotado de valor, ¿emitido por un tercero?, y con una expectativa de rendimiento. Como se puede ver, a las preguntas tradicionales del *Howey Test*, concurren respuesta afirmativa a todas, salvo en el caso de la identificación del emisor o responsable de la emisión del valor. Es por eso que la SEC en su resolución n.º 8120725 de julio de 2017, propone modificar la normativa de inclusión y centrarse en la función real de las criptomonedas como Security, más que en su noción formal, para otorgarle un tratamiento parejo al de un título valor (impropio añadido yo), e incluir expresamente en el art. 2 a) de la Securities Act y en la sec 3 de la Exchange Act, como contratos de inversión, la actividad de las compañías de «trading» en criptomonedas. Una vez más, sin embargo, se propone dejar fuera del ámbito regulatorio las operaciones *Over the Counter*, es decir, las transacciones *peer to peer* entre particulares y entre estos y las empresas de venta que admiten pagos en criptomoneda como Microsoft. El régimen tutelar se propone para las compañías que desarrollan o contribuyen a la función especulativa.

Mucho más sencillo es determinar si para el sistema bursátil las criptomonedas son un valor o activo subyacente en sentido material sobre el que se puedan crear instrumentos financieros derivados. La respuesta la da la Bolsa de Chicago, que ha sido la primera en admitir a cotización Futuros y CF sobre Bitcoins.

En otro orden de cosas, también conviene llamar la atención sobre la ordenance francesa n.º 1674, 8 diciembre 2017, en la que se admite la utilización de sistemas de compensación de valores con tecnología Blockchain, equiparando los efectos de la inclusión en el bloque a los efectos de la anotación contable por el responsable del registro de anotaciones ordinario (L211-3 Code monétaire et financier), si bien conviene matizar, que los sistemas de compensación Blockchain sólo se aplicarán a valores no cotizados en el mercado oficial, y que no se autorizan sistemas descentralizados y abiertos (DAO), sino sistemas permitidos, cerrados conducidos por un manager (DTL).

Si acudimos ya a la normativa española y comunitaria, nuestro sistema es mucho más formal que el norteamericano y nuestra legislación actual presenta graves problemas de inclusión, no tanto por la función subyacente a la operativa, como por las definiciones altamente formalizadas de nuestra ley. Así, para nuestro Art. 2 LMV «son valores negociables los emitidos por personas o entidades, públicas o privadas, y agrupados en emisiones. Tendrá la consideración de valor negociable cualquier derecho de contenido patrimonial, cualquiera que sea su denominación, que por su configuración jurídica propia y régimen de transmisión, sea susceptible de tráfico generalizado e impersonal en un mercado financiero». El problema, una vez más es que la estricta noción formal del emisor y de las series de emisión, hacen imposible encuadrar a los mineros en los criterios utilizados para la identificación de emisores del sistema euronext-alternext. La solución (parcial) a

este obstáculo formal residiría en el propio precepto, letra K, cuando permite calificar como valor «Los demás a los que las disposiciones legales o reglamentarias atribuyan la condición de valor negociable», pero está claro que, pese al enunciado de libertad de emisión de valores del art. 33 LMV, esto nos obligaría a modificar también múltiples reglas sobre la emisión de valores para incluir la negociación de criptomonedas en el art 3 LMV, como otros instrumentos financieros, y superar las barreras de inadaptación del supuesto a lo dispuesto en el art. 3 LMV (ámbito normativo), art. 7 LMV (documento de emisión), art. 34 LMV (folleto informativo), art. 8 (entidad encargada del registro contable), etc. y que la situación de hecho tropieza frontalmente con lo dispuestos en el Reglamento 600/2014 (MIFIR)⁵⁸ y en el Real Decreto-ley 21/2017, de 29 de diciembre, de medidas urgentes para la adaptación del derecho español a la normativa de la Unión Europea en materia del mercado de valores, por cuyo tenor los centros de negociación de instrumentos financieros requieren autorización, registro y organismo rector.

Nada impide a mi juicio, sin embargo, que se puedan **articular opciones o futuros** o contratos por diferenciales, como instrumentos financieros derivados que tomen por objeto o activo subyacente las criptomonedas, del mismo modo que no veo obstáculo alguno a admitir la tecnología de registro Blockchain (Distributive Ledger) en los sistemas de contratación organizada o sistemas multilaterales de contratación reconocidos por la CNMV como sistema de compensación o liquidación.

La respuesta en todo caso a la inclusión de las criptomonedas en el mercado primario o de emisión o en el mercado secundario oficial, como valor de cotización directa y no como activo derivado, es que, hoy por hoy, exigiría modificaciones sustantivas de nuestra legislación.

Queda, sin embargo, por aclarar si la actividad de negociación y promoción de venta de criptomonedas a cambio de comisión es calificable como actividad propia de **empresas de servicios de inversión** del art. 138 LMV. Y consecuentemente, si la venta de criptomonedas por estas compañías se sujetaría, al menos, a las cargas informativas a la clientela de la MIFID II.⁵⁹ Nuevamente la respuesta es, inicialmente, no, dado que el propio art. 138.1 reduce la actividad de servicios de inversión a aquellas empresas cuya actividad principal consiste en prestar servicios de inversión, con carácter profesional, a terceros sobre los instrumentos financieros señalados en el artículo 2. La remisión al art. 2 implica, inicialmente y hasta la modificación de la norma, una exclusión inmediata de las agencias de inversión (exclusivamente) en criptomonedas, pese a que las actividades funcionales de dichas empresas sean materialmente coincidentes con las ofertadas en el mercado oficial (art. 140 LMV). Si miramos en la Directiva MIFID II la definición de empresa de

58. REGLAMENTO (UE) No 600/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de mayo de 2014 relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) no 648/2012.

59. Directiva UE 2014/64 de 15 de mayo relativa a los mercados de instrumentos financieros que mejor las reglas de la MIFID I y establece las reglas de autorización y funcionamiento de las empresas de servicios de inversión y las normas de protección del inversor

servicios de inversión⁶⁰, y la obligatoriedad de autorización del art. 5, nuevamente, plantea un problema de encuadramiento formal de la mayor parte de los agentes mediadores en criptomonedas. Ahora bien, dándole la vuelta al razonamiento; no veo obstáculo a que las empresas de servicios de inversión oficiales, ofertaran entre su cartera de inversiones la inversión en criptomonedas, salvando las cautelas de información relativas a la ausencia de garantías que implica el instrumento financiero y avisando de su volatilidad y falta de garantías (no cobertura por el fondo de garantía de inversiones o de depósitos), si nos referimos a un instrumento como Bitcoin. A día de hoy, sin embargo, las ESI, sistemas multilaterales de negociación y sistemas organizados de contratación hacen vida aparte de la negociación en bitcoins, ethers y similares y para la CNMV la mayor parte de los agentes en bitcoins aparecen registrados en la lista no exhaustiva de «Advertencias: Otras entidades»⁶¹, sobre las que se predica «que no cuentan con ningún tipo de autorización ni están registradas a ningún efecto en la CNMV y que podrían estar realizando algún tipo de actividad de captación de fondos o prestando algún servicio de naturaleza financiera», si bien, «La inclusión en la lista no implica pronunciamiento alguno sobre la conformidad o no con la normativa vigente de la posible actividad de las correspondientes entidades». Es decir, no se las señala directamente como compañías fraudulentas de la lista de «chiringuitos financieros»⁶².

Y dicho esto, mientras el sistema europeo medita sobre cómo abordar este fenómeno híbrido y ciertamente disruptivo con las reglas del sistema, vemos como proliferan las agencias que ofrecen «inversiones» en Bitcoins, ofrecen cursos sobre especulación en el «mercado» de Bitcoins, y obtienen comisiones de intermediación y gestión de carteras sin someterse a la normativa tutelar de cualquier agente de servicio de inversión del mercado oficial. Tampoco hay que rasgarse las vestiduras si pensamos que los inversores en criptomonedas normalmente buscan una inversión de alto riesgo y no se han preocupado por el respaldo legal de las mismas o son conscientes del carácter atípico de la inversión. Pero el problema es que, sin duda, muchos de estos inversores desconocen el alcance real de su opción, ya que no se les ha proporcionado un nivel de información precontractual equiparable al de las inversiones normalizadas. Las notas de advertencia emitidas por el Banco de España y la CNMV, serán un triste consuelo para muchos de los «inversores» captados por estos agentes, si llegan a verse involucrados en un fiasco.

60. «toda persona jurídica cuya profesión o actividad habituales consisten en prestar uno o más servicios de inversión o en realizar una o más actividades de inversión con carácter profesional a terceros. Los Estados miembros podrán incluir en la definición de empresa de servicios de inversión a empresas que no sean personas jurídicas, siempre que: a) su estatuto jurídico garantice a los intereses de terceros un nivel de protección equivalente al que ofrecen las personas jurídicas, y b) sean objeto de una supervisión prudencial equivalente y adaptada a su forma jurídica».

61. http://www.cnmv.es/docportal/aldia/Advertencias_CNMV_Otras.pdf

62. <http://www.cnmv.es/docportal/Publicaciones/Guias/chiringuitos.pdf>

5. RÉGIMEN JURÍDICO DE LOS PAGOS EN CRIPTOMONEDAS VIRTUALES

Por otro lado, dejando al margen la calificación del pago en criptomoneda como instrumento de pago en sentido propio, con el pago en divisa virtual propiamente estamos ante una permuta de valor de un bien fungible (art. 337 C.C.), la representación digital de un valor de cambio aceptable como medio de pago mediando consentimiento y aceptación de las partes (art. 1.166 C.C.) y con sometimiento a lo dispuesto en el art. 1170.2 del C.C. (medio de pago pro solvendo «salvo buen fin») a los efectos de fijar el momento solutorio⁶³. Y por ello, lo que es más importante de resaltar, ante un pago perfectamente legal y eficaz en términos jurídicos (ex art. 1.166 y 1170.2 C.C.)

V. CONCLUSIONES

La incorporación del automatismo contractual a nuestro ordenamiento jurídico es sencillamente, un paso inevitable de la dinámica introducida por la aparición de la economía digital. En un plazo breve hemos asistido a la progresiva digitalización de las comunicaciones y a la automatización de las funciones económicas en las cadenas de valor (almacenes robotizados, documentos de trazabilidad, sistemas de producción *just in time*)⁶⁴ en una búsqueda de maximización de la eficiencia y de la reducción de costes operativos. La aparición de los Smart Contracts o contratos en formato electrónico autoejecutable era por ello una necesidad para dar respuesta a esa creciente búsqueda de eficacia en operaciones en masa, a la multiplicación en el ámbito electrónico de micro operaciones y a la creciente demanda de estructuración de las operaciones en el internet de las cosas. Aunque todavía quedan aspectos por armonizar, el principio de que el ordenamiento jurídico es completo y la articulación de los mecanismos de equivalencia entre los instrumentos digitales y los instrumentos de expresión física, nos lleva a que es perfectamente posible reproducir y adaptar la normativa existente a este entorno. Al menos, en lo que se refiere a la contratación utilizando Smart Contracts o contratos autoejecutables. Sigue siendo posible identificar a los sujetos responsables de las obligaciones, atribuir las responsabilidades pertinentes, identificar las leyes y foros competentes, etc. etc.

63. ¿Cuándo puede entenderse realizado el «buen fin» de este título impropio en formato digital, por utilizar la terminología de la doctrina alemana de títulos valores? A mi juicio no con la simple entrega, puesto que aun cabe el riesgo de que se nos haya colocado en una cadena de bloques improductiva (fork) que no sea reconocida por el registro, y tampoco cuando se realice un pago o conversión de la criptomoneda, puesta puede quedar almacenada como valor largos periodos y no puede hacerse depender la perfección una transacción de la realización de una operación posterior, así que el momento relevante será el correspondiente a la inclusión de la transacción en el registro definitivo o validación del bloque por los nodos del sistema.

64. ECHEBARRÍA SÁENZ, J.A., Voz «Distribución comercial» en *Diccionario de derecho de la competencia*, Velasco San Pedro, L. A. (Director), Madrid, Iustel, 2006, (Págs. 323-331), «El comercio electrónico entre empresarios» en *El comercio electrónico...*, 2001, págs. 81-144

El panorama jurídico, sin embargo, ha tropezado con un elemento inesperado, la aparición de la tecnología Blockchain, y más concretamente, con la aparición de redes autónomas descentralizadas (DAO) en las que fallan los tradicionales parámetros de atribución de responsabilidad, atribución de valor y encaje de régimen jurídico. Frente a la utilización de instrumentos como el dinero electrónico que, pese a su juventud, ya podemos calificar como instrumento de pago «tradicional», por cuanto es un instrumento regulado y respaldado por el ordenamiento, la aparición de los sistemas mutualistas infraestructurales⁶⁵ y las tecnologías de contabilidad distributiva (*distributive ledger*) se salen por las costuras de un ordenamiento que no ha contemplado el traje adecuado para este fenómeno. Tanto los entes descentralizados (DAOs)⁶⁶ como los sistemas de contabilidad compartida bajo el control y dirección de un operador tradicional (sistemas GDS)⁶⁷ permiten crear un gigantesco registro de datos de transacciones monetarias o contractuales con bajo coste, alta fiabilidad, resistencia computacional, acceso público y ahorro de costes de intermediación y transacción, aplicables a las más variadas funciones (criptomonedas, sistemas de compensación, bases de datos de siniestros, atribución de cuotas de generación eléctrica, funciones de información pública, gestión de mercancías etc. etc.). La diferencia reside en que el primer modelo, los sistemas mutualistas descentralizados (DAO), operan sin crear una estructura jerárquica y difuminan de manera fatal los tradicionales principios de atribución de responsabilidad jurídica, a la vez que hacen prácticamente inoperativos los criterios de atribución de ley aplicable y foro competente utilizados en el Derecho Internacional.

Ciertamente, estas dificultades, y la ausencia de un estatus legal reconocido y dotado de seguridad jurídica, no priva de legalidad a las operaciones efectuadas en este tipo de plataformas, y significativamente a los pagos e inversiones realizadas en sistemas de criptomonedas, que son perfectamente legales y admisibles en Derecho. Las monedas virtuales, son perfectamente encuadrables como medio de pago y surten plenos efectos, aunque sus operadores aún no formen parte del sistema regulado. Es igualmente cierto, por el contrario, que los sistemas de criptomoneda carecen de mecanismos contra el riesgo sistémico financiero o que su propia alegación les coloca en un riesgo institucional, que es, quizás, el más grave. Asistimos, además, a un proceso de incorporación creciente de los operadores de monedas virtuales al sistema de supervisión cautelar (mercado derivado o secundario de negociación y venta de las criptomonedas). Ya disponen de un régimen fiscal, se les aplica la normativa de prevención del terrorismo y blanqueo de capitales, aun sin una declaración formal al efecto, y es cuestión de poco tiempo que se les aplique determinadas normas cautelares de la regulación de servicios de pago, si bien esta última etapa, recién iniciada, aun es incierta en su ejecución y previsiblemente tropezara tanto con la filosofía de estas redes, como con su estructuración

65. SWARTZ, «El sueño del Blockchain...» págs. 127.

66. SWARTZ, «El sueño del Blockchain...» págs. 129 y ss

67. Caso de la *distributive ledger initiative* 2015 fomentada por los 15 bancos principales del mundo en ordena crear un sistema de moneda virtual propia y un sistema de compensación y liquidación de operaciones globalizado basado en tecnología blockchain. SWARTZ, «El sueño del Blockchain...». Págs.. 129 y ss

como sistema anónimo, que entra por ello en contradicción con la normativa de supervisión comunitaria. Más lejos está la adaptación de las «inversiones» en criptomonedas al sistema de servicios financieros. En todo caso, y con independencia de cómo lleguen a solucionarse estos encuadramientos, el principal problema de las divisas virtuales para articular sistemas de contratación fiables, estandarizados y continuados en el tiempo, es su propia volatilidad. El hecho de que actúen simultáneamente como unidad de valor y como valor especulativo, al punto de que ningún sistema de contratación automatizada puede articularse sobre una unidad de cuenta cuyo valor es indeterminable por su rápida fluctuación. Esto limita la funcionalidad de la divisa virtual a operaciones aisladas y la aleja de posibles contratos marco para operaciones en serie.

Finalizo con una reflexión de Anthony Giddens, animémonos a «ocupar el futuro» e imaginar sistemas innovadores. Solucionemos razonablemente los problemas y abramos nuevos sectores económicos, pues de otro modo ya llegará quien nos escriba el futuro según sus intereses.

VI. BIBLIOGRAFÍA Y REFERENCIAS WEB

- AA.VV. «Bower-Christensen, Disrupting Technologies: Catching the Wave», in *Harvard Business Review*, I, 1995, 43
- AA.VV. CALVO CARAVACA, A./CARRASCOSA GONZÁLEZ, J. «Problemas de extraterritorialidad en la contratación electrónica» en ECHEBARRÍA SÁENZ, J. (Dir) *El comercio electrónico*, págs. 145-217.
- AA.VV., «COLLABORATION OR BUSINESS? From value for users to a society with values», Madrid, OCU, Creative Commons, 2017.
- AA.VV., BÖHME-CHRISTIN-EDELMAN-MOORE, «Bitcoin: Economics, Technology and Governance», in *Journal of Economic Perspectives*, Vol. 29, n. 2, 2015, 213.
- AA.VV., MATA MARTÍN, R./JAVATO MARTÍN, A. *Los medios electrónicos de pago*, Granada Comáres, 2007
- AA.VV., POLASIK-PIOTROWSKA-WISNIEWSKI-KOTKOWSKI-LIGHTFOOT, «Price Fluctuation and the use of Bitcoin», en *International Journal of Electronic Commerce*, Vol. 20, n. 1, 2016, 9.
- AA.VV., VELASCO, ECHEBARRÍA, HERRERO (Dir) *Acuerdos horizontales, mercados electrónico y otras cuestiones actuales de competencia y distribución*, Valladolid, Lex Nova Thomsom-Reuters, 2014.
- AAVV., PEREIRA DE ARAÚJO, H./ARAMBASIC REBELO DA SILVA, R.B. «A TECNOLOGIA DIGITAL BLOCKCHAIN: ANÁLISE EVOLUTIVA E PRAGMÁTICA», en *REFAS* v3, n.º 4, junio 2017 (ISSN 2359-182X).
- ALVARADO HERRERA, L. «El servicio de iniciación de pagos en la Directiva 2015/2366 sobre servicios de pago en el mercado interior» en *La Ley mercantil* n.º 34, 2893 2017

- BBVA Research, «Smart Contracts: ¿lo último en automatización de la confianza» en CASTELLS, M. et al. *Otra economía es posible. Cultura y economía en tiempos de crisis*. Alianza editorial, Madrid, 2017.
- BITCOIN. <https://elbitcoin.org/escenarios-posibles-partir-del-fork/>
- BITCOIN. www.bitcoinfoundation.org
- BLOCKCHAIN. <https://blockchain.info/en/charts/market-cap>
- BOLSAMANIA. www.bolsamania.com/noticias/tecnología/que-es-el-une-te-una-estafa-de-50-millones-de-euros-a-partir-del-bitcoin-de-jose-manuel-ramirez--771685.html
- BONET CORREA, J. *Las deudas de dinero*, Madrid, Civitas, 1981.
- CHERNUKKA, V., «Como influencia el hard fork al precio del bitcoin» <https://blog.iqoption.com/como-influencia-el-hard-fork-al-precio-del-bitcoin/30-10-2017>
- COINDESK. <https://www.coindesk.com/bitcoin-cash-developers-set-date-november-hard-fork/>
- COINTELEGRAPH. <https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-qu%C3%A9-consisten-y-cu%C3%A1les-son-sus-diferencias>
- COMISIÓN EUROPEA. Libro Verde, «Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por internet o pagos móviles» 11 de enero de 2012.
- CRIPOTENDENCIA. <https://criptotendencia.com/2017/09/29/primerocash-ahora-gold-otro-hard-fork-de-bitcoin-esta-en-camino/>
- CUCCURU, Pierluigi. «Blockchain ed Automazione contrattuale. Riflessioni sugli smart contract» WOLTERS Kluwer Italia, 2016.
- EBA. European Central Bank, *Opinion on virtual currencies*, Report, 4.7.2014, in www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+
- EBA. European Central Bank, *Virtual Currency Schemes*, Report, octubre 2012, in www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
- ECHEBARRÍA SÁENZ, J. A. «La carta de porte emitida electrónicamente» en Comentarios a la ley de transporte terrestre, DUQUE DOMÍNGUEZ, J/MARTÍNEZ SANZ, F. (Dir.) Aranzadi Thomson-Reuters, Pamplona 2010, ISBN 978-84-9903-629-8, págs. 185-212
- ECHEBARRÍA SÁENZ, J. A. (Dir) *El comercio electrónico*, Madrid, Edisofer, 2001
- ECHEBARRÍA SÁENZ, J. A., «El dinero electrónico; construcción del régimen jurídico emisor-portador» en MATA/JAVATO, Los medios electrónicos de pago, Granada, Comares, 2007, págs. 219-267.
- ECHEBARRÍA SÁENZ, J. A., Voz «Distribución comercial» en *Diccionario de derecho de la competencia*, Velasco San Pedro, L. A. (Director), Madrid, Iustel, 2006, Págs. 323-331.

- ECHEBARRÍA SÁENZ, M., «Contratos electrónicos autoejecutables (Smart contract) y pagos con tecnología Blockchain» en REE número monográfico Economía colaborativa, 2, diciembre 2017, ISSN: 2530-9854. <http://www.ree-uva.es/>
- El Diario. http://www.eldiario.es/hojaderouter/seguridad/seguridad-carteras-bitcoin-hackers-criptomonedas_0_363264145.html
- European Banking Authority, Opinion on «virtual currencies», 4th July 2014
- FATF (GAFI). *Guidance for a risk-based approach, Virtual Currencies*, 2015
- Financial Action Task Force (FATF-GAFI), VIRTUAL CURRENCIES – KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS, 2014
- FORBES. <https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#a742865337d4>
- GARCIA, R./VASQUEZ, C., «Supercalifragilisticoespialidoso... perdón, quería decir Blockchain», en *Espacio Actuarial*, n.º 39, otoño 2016.
- GORJÓN, S., Banco de España, Eurosistema, Dirección General de Operaciones, Mercados y Sistemas de Pago», Divisas o Monedas Virtual: El caso de Bitcoin» ENERO 2014, Pág. 4/13
- GURUSBLOG. www.gurusblog.com/archives/bitcoin-al-borde-del-colapso-tecnico/06/03/2016/
- LÓPEZ LÉRIDA J., «Las tecnologías Blockchain», en Agenda de la empresa, junio 2017
- NAKAMOTO SATOSHI, «Bitcoin: a peer to peer electronic cash system», 2009. www.bitcoinfoundation.org
- NUSSBAUM, *Teoría jurídica del dinero*, Madrid, 1929 (Traducción Sancho Seral).
- O'REILLY. *Blockchain: blue print for a new economy*, Swan, 2015
- Oermann-Töllner, The Evolution of Governance Structure in Cryptocurrencies and the Emergence of Code-Based Arbitration, https://cyber.harvard.edu/publications/2014/internet_governance_in_Bitcoin_on+Virtual+Currencies.pdf
- OPEN TRANSACTIONS. http://opentransactions.org/wiki/index.php/Voting_Pools
- Oro y Finanzas. <https://www.oroymasfinanzas.com/2014/11/definicion-bitcoin-2-0-que-es-bitcoin-2-0/>
- Oro y Finanzas. <https://www.oroymasfinanzas.com/2015/07/ethereum-proyecto-bitcoin-2-0-mas-ambicioso-lanza-plataforma-descentralizada-frontier/>
- Oro y Finanzas. <https://www.oroymasfinanzas.com/2015/10/rootstock-contratos-inteligentes-smart-contracts-ethereum-bitcoin/>

Oroy Finanzas. <https://www.oroynfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/>

Oro y Finanzas. <https://www.oroynfinanzas.com/2015/04/aplica-ley-prevencion-blanqueo-capitales-bitcoin-espana/>

RAMOS SUAREZ, F. (Presentación) LA REGULACIÓN JURÍDICA DE LAS MONEDAS VIRTUALES Y LA TECNOLOGÍA BLOCKCHAIN, Fide DPO it Law, mayo 2016-

Regulation of bitcoin in selected jurisdictions: <http://www.loc.gov/law/help/bitcoin-survey/>

Situación Economía Digital, Octubre 2015.

SWARTZ, LANA, «El sueño del Blockchain. Imaginando alternativas tecnoeconómicas más allá del bitcoin» en CASTELLS, M. et al. *Otra economía es posible. Cultura y economía en tiempos de crisis*. Alianza editorial, Madrid, 2017, págs. 123-155.

Technology review. <http://www.technologyreview.es/informatica/44368/escribe-la-clave-de-tus-bitcoins-en-un-papel-si/>

U.S. Congress, Bitcoin: Questions, Answers, and Analysis of Legal Issues: <https://fas.org/sgp/crs/misc/>

UK Treasury, Digital Currencies: Response to the Call of Information, Report, marzo 2015: www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

VICENTE BLANCO, D. J. «Medios electrónicos de pago y jurisdicción competente en supuesto de contratos transfronterizos en Europa», en MATA MARTÍN, R./JAVATO MARTÍN, A. *Los medios electrónicos de pago*, Granada, Comares, 2007, págs. 270-319.

VICENTE BLANCO, D. J. «Problemas de jurisdicción competente y ley aplicable en los mercados electrónicos» en VELASCO, ECHEBARRÍA, HERRERO (Dir) *Acuerdos horizontales, mercados electrónico y otras cuestiones actuales de competencia y distribución*, Valladolid, Lex Nova Thomson-Reuters, 2014, págs. 644-666.

VICENTE BLANCO, D. J. «Medios electrónicos de pago y jurisdicción competente en supuesto de contratos transfronterizos en Europa», en MATA MARTÍN, R./JAVATO MARTÍN, A. *Los medios electrónicos de pago*, págs. 270-319.

XATAKA. <https://www.xataka.com/empresas-y-economia/mas-forks-de-bitcoin-mas-incertidumbre-a-bitcoin-cash-se-le-suman-bitcoin-gold-y-el-segwit2x>

YUAN, L., «Forget bitcoin, Long live Blockchain» 2015