Revista de Derecho Civil
http://nreg.es/ojs/index.php/RDC
ISSN 2341-2216
vol. VI, núm. 1 (enero-marzo, 2019)
Estudios, pp. 177-237

# RETOS JURÍDICOS QUE PLANTEA LA TECNOLOGÍA DE LA CADENA DE BLOQUES. ASPECTOS LEGALES DE *BLOCKCHAIN*

*Antonio Legerén-Molina*

Profesor Contratado-Doctor Derecho civil
Universidade da Coruña

---

TITLE: *Legal challenges about blockchain.*

RESUMEN: Entre las herramientas tecnológicas que actualmente suscitan mayor interés se encuentran las cadenas de bloques. Desde que en 2009 se crease la conocida como *Blockchain*, no son pocas las que han ido apareciendo con posterioridad. Según se indica, esta novedosa tecnología permite eliminar intermediarios, pero garantizando –e incluso aumentando– la seguridad que aquellos proporcionaban, a la vez que incrementa la eficiencia y reduce costes. Como toda tecnología novedosa, tiene que resolver o encauzar los problemas jurídicos que suscita su uso. El presente artículo pretende abordar algunos de los retos que plantean las cadenas de bloques de carácter público –en especial, *Blockchain*–: la falta de dueño, los límites de la función registral que desarrolla, algunos aspectos sobre la identidad de los intervinientes, o la caracterización de las criptomonedas y su relación con los impuestos o el dinero legal. Finalmente, también se hace mención a los *smart contracts* con relevancia jurídica que se ejecutan utilizando esta tecnología.

ABSTRACT: *Among those technological tools which currently trigger great interest are so-called «blockchains». Since the launch of Blockchain in 2009, many such systems have been devised. As is apparent, this technology tends to eliminate intermediaries, while guaranteeing and even increase the security they provide. At the same time, it improves efficiency while reducing costs. Like any other new technology, it must address the legal challenges that arise from its use. The goal of this paper is to address some of those referred to public blockchains –specially, Blockchain–, to wit: the lack of ownership, the limits of their registry functions, concerns regarding the identity of the participants, the character of cryptocurrencies and their relationship to tax structure or legal money, and finally, the legal smart contracts that can be executed using this technology*.

PALABRAS CLAVE: Cadena de bloques, *Blockchain*, criptomonedas, *bitcoin*, función de registro, contratos inteligentes, sellado de tiempo.

KEYWORDS: *Blockchain, Blockchain, cryptocurrencies, bitcoin, register function, smart contracts, time-stamp*.



---

## 1. INTRODUCCIÓN

En los últimos meses, el término «*blockchain*» –en castellano, «cadena de bloques»– se ha convertido en parte del lenguaje común –y del «lenguaje de moda»– de muchos ciudadanos. Ahora mismo, cualquier buscador de internet arroja cientos de miles de entradas sobre él. Como es conocido, se trata de una «tecnología» en auge, que, ciertamente, puede generar un nuevo modo de trabajar con seguridad y sin necesidad de recurrir a intermediarios. Es más, se ha dicho que es una «nueva filosofía», una nueva metodología de trabajo que pretende positivamente prescindir de los intermediarios que sean considerados innecesarios, pero garantizando la misma o mayor seguridad que la que ofrecen éstos[1]. Como toda «tecnología» novedosa tiene que resolver o encauzar los problemas jurídicos que suscita su uso. El presente artículo pretende abordar algunos de los retos que plantean las cadenas de bloques de carácter público –en especial, de *Blockchain*–: la falta de dueño, los límites de la función registral que desarrollan, algunos aspectos sobre la identidad de los intervinientes, o la caracterización de las criptomonedas y su relación con los impuestos o el dinero legal, entre otros.

Asimismo, una vez se efectúe el análisis de lo señalado, examinaremos algunas cuestiones que suscitan los *smart contracts* con relevancia jurídica que se ejecutan utilizando esta tecnología: su «inmutabilidad», su carácter autoejecutable o su necesario carácter objetivo. Ahora bien, a fin de comprender el alcance de los problemas apuntados, parece preciso comenzar con una explicación del concepto y los caracteres de la cadena de bloques (apartado 2), de su funcionamiento (apartado 3), así como de las ventajas e inconvenientes que la caracterizan (apartado 4).

## 2. LA CADENA DE BLOQUES: CONCEPTO Y CARACTERÍSTICAS

Cabe afirmar que la cadena de bloques, tal y como ahora la concebimos, vio la luz en el año 2009. SATOSHI NAKAMOTO fue quien dio a conocer la primera cadena –que denominó

[1] En efecto, según se verá, el uso de criptomonedas –p. ej., *bitcoin*– puede ser un incentivo para el desarrollo de una actividad empresarial por su carácter descentralizado, desintermediado –evita comisiones–, transnacional, e inmutable, al estar incluida en una cadena de bloques. De todos modos –y como también se verá– la regulación existente en este campo es escasa, y la seguridad jurídica constituye un elemento importante para el desarrollo de las mencionadas actividades. Por otra parte, aunque en el fondo las cadenas de bloques constituyen una metodología de trabajo para dar confianza, nos referiremos a ellas con el término «tecnología» pues simplifica la redacción, la hace más inteligible y evita reiteraciones innecesarias. En sí mismas, las cadenas de bloques no son un software, ni son un protocolo, aunque usen ambos.

*Blockchain*– y la criptomoneda que soporta, llamada *bitcoin*[2]. Aunque la mencionada sea quizá la más conocida –y la más controvertida– y soporte esa específica criptomoneda, una cadena de bloques puede configurarse con características distintas a las de *Blockchain*. En efecto, tal «tecnología» en sí misma no resulta controvertida, y buena prueba de ello es que actualmente existen: cadenas públicas donde cualquier usuario puede añadir «bloques» o leer lo registrado; cadenas privadas en las que la escritura está abierta solo a sus miembros y el acceso y la lectura pueden estar configuradas de la misma manera o ser más público; y cadenas híbridas[3]. Igualmente,

[2] El nombre de «criptomoneda» deriva del hecho de que solo la persona que conozca la clave criptográfica que da acceso a ella es quien la puede usar o puede disponer de ella. No tiene un soporte papel ni consistencia material; únicamente informática pues se trata de «mera información digital». O dicho de manera técnicamente más precisa: solo puede disponer de la criptomoneda quien conoce la clave criptográfica *privada* que está vinculada a la clave *pública* del que ha sido beneficiario de una transacción anterior; materia sobre la que en breve volveremos. A lo que parece, aun cuando factores técnicos, sistémicos, especulativos e institucionales imposibilitaran su desarrollo, el intento de crear «monedas virtuales» se remonta a la década de los 80-90 del pasado siglo (cfr. ECHEBARRÍA SÁENZ, «Contratos electrónicos autoejecutables (*smart contract*) y pagos con tecnología *blockchain*», *Revista de Estudios Europeos*, nº 70, julio-diciembre, 2017, p. 81). De los intentos de entonces, quizá los más conocidos sean los de DAVID CHAUM en 1982 cuando introdujo el *E-cash scheme* o el de WEI DAI, quien en 1998 sentó las bases de un sistema no centralizado de carácter cooperativo en el que se contemplaba la creación de dinero –*b-money*– y su transacción por medio del uso de la criptografía. Respecto del creador de *Blockchain* –SATOSHI NAKAMOTO–, es común señalar que su identidad real no es conocida y que un *satoshi* es como se denomina a la mínima parte en que se puede dividir un *bitcoin*: una cien millonésima parte de él. Finalmente, cabe advertir ahora que, en el presente trabajo, se distingue *bitcoin* (BTC) como unidad monetaria individual y *Bitcoin* como el sistema que soporta dicha criptomoneda, y *Blockchain* como la cadena de bloques específica de tal nombre, y *blockchain* como un genérico referido a las cadenas de bloques. Asimismo, conviene también recordar de nuevo que nos referiremos fundamentalmente a las cadenas de bloques de carácter público, y la mayor parte de lo que se dirá es referible a las distintas criptomonedas actualmente existentes, aun cuando su estudio –así como el del funcionamiento de las cadenas de bloques– se realice sobre la base del *sistema Bitcoin* –*Blockchain*– y la criptomoneda *Bitcoin*. Y, por último, reseñamos que algunas de las citas se incluyen en inglés, pues entendemos que reflejan mejor su contenido que la eventual traducción al castellano. En otros casos, la traducción es de nuestra autoría.

[3] Algunos ejemplos de las primeras cadenas son *Everledger* (https://www.everledger.io) o *Etherisc* (https://etherisc.com). Quizá la que actualmente revista mayor interés –de manera especial por lo que a los *smart contracts* o «contratos inteligentes» se refiere– es *Ethereum*; plataforma de computación descentralizada basada en una cadena de bloques pública y en código abierto, creada en 2014 por VITALIK BUTERIN (https://www.ethereum.org/). Lo más específico de Ethereum es que permite la ejecución de *smart contracts* en una plataforma virtual descentralizada –denominada *Ethereum Virtual Machine*– y usa un lenguaje de programación más completo que el *sistema Bitcoin* y que es Turing completo. La criptomoneda que se apoya en esta cadena es el *Ether*, auque tras el *fork* de 2016 –concepto que luego se explicará– se dividió en dos criptomonedas: *Ethereum* (ETH) y *Ethereum Classic* (ETC). Así las cosas, y aun cuando las cadenas de bloques resulten un instrumento útil para las de carácter privado –denominadas con frecuencia como DLT por sus siglas en inglés: *distributed ledger technology*–, hay que señalar que, en cierta medida, tales cadenas contradicen la idea inicial a que responde la creación de dicha herramienta pues el *sistema Bitcoin* pretendía ser un sistema alternativo de pagos al establecido, totalmente abierto, independiente y sin intermediarios (cfr. GONZÁLEZ-MENESES, *Entender Blockchain, Una introducción a la tecnología de registro distribuido*, Thomson Reuters Aranzadi, Cizur Menor, 2017, p.

las cadenas de bloques soportan *tokens* de diverso tipo que pueden servir para albergar criptomonedas –p. ej., *bitcoin*– u otros criptoactivos[4]. La expansión de la «tecnología» a que aludimos –que, generalmente toma el nombre de la primera cadena de bloques– se debe a que es una metodología versátil, es una herramienta rápida y, fundamentalmente, reduce costes al no haber intermediarios, a la vez que da seguridad y confianza, pues elimina la posibilidad de manipular los datos registrados en ella[5]. Razones que han impulsado a empresas privadas y corporaciones públicas a

37). La limitación o control de los derechos de acceso, lectura y escritura en una cadena de carácter privado, necesariamente remiten a un órgano supervisor y van «en contra» del carácter descentralizado: alguien ha de determinar, por ejemplo, tales derechos. Un resumen esquemático de las diferencias entre los distintos tipos de cadenas mencionados se recoge en PREUKSCHAT, «Los fundamentos de la tecnología *blockchain*», en VV AA, *Blockchain: la revolución industrial de internet* –coord. PREUKSCHAT–, Gestión 2000, Barcelona, 2017, pp. 27-30. Por otra parte, las que hemos calificado como híbridas se caracterizan porque todas las «transacciones» son públicas pero los nodos participantes son «invitados» –p. ej. pueden ser tales las instituciones públicas–. Dos ejemplos son BigchainDB (https://www.bigchaindb.com) o Evernym (https://www.evernym.com). Asimismo, y junto con el binomio pública-privada, también existe el de redes permisionadas («*permissioned*») y sin permiso («*permissionless*») que aluden fundamentalmente a los derechos de validación o registro de datos (sobre él, vid. IBAÑEZ JIMÉNEZ, *Derecho de blockchain y de la tecnología de registros distribuido*, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 53-54). Por otra parte, calificando como públicas las cadenas de bloques «*permissionless*» vid., FINCK, M., «Blockchain regulation», *German Law Journal*, 2018, *Max Planck Institute for Innovation & Competition Research* Paper nº 17-13, http://dx.doi.org/10.2139/ssrn.3014641, p. 4.

[4] El llamado proceso de «tokenización» supone representar en digital cualquier bien del «mundo físico»; es, por tanto, una representación abstracta del valor. Así, en una cadena de bloques se puede incluir cualquier cosa susceptible de ser registrada en ella, ya sean bienes físicos –el oro o propiedades inmobiliarias–, derechos incorporales o intangibles como las criptomonedas, transacciones e instrumentos financieros o registros con información de ciudadanos (cfr. KEMP, «Legal Aspects of Artificial Intelligence», 22 num. 1 *Cyberspace Lawyer NL* 2, January-February 2017, nº 19; mostrando dudas, desde la perspectiva de los efectos jurídicos, sobre la posibilidad de que *cualquier cosa* pueda ser transferida usando *blockchain*, vid. ARRUÑADA, «Blockchain's Struggle to Deliver Impersonal Exchange», *Minnesota Journal of Law, Science & Technology*, vol. 19, 1, 2018, p. 86). En efecto, cuestión distinta a la mera posibilidad técnica de «tokenizar» algo es la eficacia jurídica que se le reconozca fuera de internet al intercambio o transmisión de bienes «tokenizados». Dentro de los tokens, los más conocidos son las criptomonedas y las *appcoins*. Estas últimas dan un derecho de consumo o adquisición de un bien o servicio. Sobre la legislación que les resulta aplicable vid. OTERO MOREIRAS, «Los tokens vistos por un abogado», 11 de octubre de 2017, https://bit.ly/2VrAB4j y MORA, «Las ICOs no están reguladas ¿o sí? Análisis jurídico de la token-economía», 13 de octubre de 2018, https://bit.ly/2BYMHJi. De otra parte, anunciamos ahora que en el texto explicaremos únicamente el significado de algunos de los términos más importantes relativos a las cadenas de bloques; para tener una visión completa de la terminología al uso vid. http://blockchainespana.com/glosario/.

[5] Vid., TAPSCOTT & TAPSCOTT, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, Penguin Random House, 2016, pp. 17-20 y 60-61, quienes mencionan algunas de las ventajas de la tecnología *blockchain* que cabe resumir de la siguiente forma: «adding improved attestation, dramatically lower costs, lighting speed, lower risks, greater innovation of value, and improved adaptability for the investment banking, insurance, accounting and retail banking industries». MCJOHN y MCJOHN («The Commercial Law of Bitcoin and Blockchain Transactions», 47 num. 2 *Uniform Commercial Code Law Journal ART 4*, July 2017) mencionan también como ventaja de las DLT la transparencia que proporcionan al tener cada usuario una copia de toda la base de datos, su carácter abierto –accesible para todos los que quieran usar el sistema– y que permiten hacer rápida y sencillamente las transacciones. Por otra parte, y respecto de la trascendencia de las cadenas de bloques

explorar sus posibilidades de uso[6]. Las ventajas señaladas son consecuencia de las dos principales características de esta «tecnología»: ser una base de datos *online* de carácter descentralizado.

En efecto, una cadena de bloques es una base de datos *online* única y descentralizada que puede contener cualquier tipo de registro: es como un libro de contabilidad único –un *ledger*– donde se van efectuando apuntes. Su carácter único en conexión con su carácter descentralizado hace que *toda* la base de datos esté *guardada* en cada uno de los ordenadores que forman parte de la cadena –los llamados «nodos»–. No está, por tanto, centralizada bajo una sola autoridad o servidor ni se guarda una porción de ella en cada sitio, sino que hay una copia de toda ella en todos y cada uno de los ordenadores que son parte de la cadena. Esta es la razón de que su manipulación resulte casi imposible: habría de alterarse el contenido en todos y cada uno de los nodos que contienen una copia de la base de datos[7].

---

en el mundo actual se ha dicho que son la «tercera revolución tecnológica», comparable al cambio generado por el propio internet, en atención a la multiplicidad de usos que permite (cfr. DUIVESTEIN y SAVALLE, «Bitcoin: It's the platform, not the currency, stupid!», 15 de febrero de 2014, https://bit.ly/2VsFOsA). Es más, se habla ya de la existencia de un *blockchain* 2.0 unido al «internet de las cosas» y a los *smart contracts* (cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 112). El tiempo dirá si tal apreciación es cierta o no.

[6] Sería imposible dar noticia aquí de las innumerables iniciativas existentes en relación a las cadenas de bloques. Señalamos solo algunas que nos parecen particularmente interesantes. Entre otros países que están desarrollando la tecnología DLT a nivel institucional, cabe mencionar a Dubai –pretende tenerla implantada a nivel gubernamental en 2020–, Estonia –quiere aplicarla para almacenar los datos de su sistema público de salud– o Suecia, Honduras y Georgia –que trabajan para su aplicación en el ámbito inmobiliario– (una crítica de la propuesta inmobiliaria sueca de cadenas de bloques se recoge en ARRUÑADA, «Limitaciones de *blockchain* en contratos y propiedad», *Revista Crítica de Derecho Inmobiliario*, nº 769, 2018, pp. 2479 a 2481 y 2487 a 2488). En el ámbito privado, basta ahora aludir a: «Initiative B3i», cadena de bloques iniciada en octubre de 2016 para aumentar la eficiencia en el intercambio de datos entre las compañías de seguros y reaseguros (https://b3i.tech/home.html); a Alastria (https://alastria.io/#1), cadena de bloques española de carácter multisectorial que engloba a importantes empresas; al programa común iniciado en junio de 2017 entre AIG e IBM para desarrollar un «contrato inteligente» que use la tecnología de las cadenas de bloques en la gestión de coberturas internacionales (https://ibm.co/2Szd0gd); a Wien Energie para el intercambio de energía entre empresas de dicho sector en Austria (https://bit.ly/2R3jXJL), o, finalmente, y en otro marco, la Woolf University desarrollada en Oxford en marzo de 2018, que pretende ser la primera universidad construida sobre la tecnología *blockchain* (https://woolf.university/#/). Asimismo, son varias las plataformas que permiten la creación de cadenas de bloques privadas; vid. por todas, *Quorum* o *Hyperledger* (https://www.hyperledger.org). Mencionados los ejemplos anteriores, cabe advertir que uno de los ámbitos donde más iniciativas existen respecto de las cadenas de bloques es el financiero. Sobre esta cuestión, vid. EUROPEAN CENTRAL BANK, *Virtual currency schemes*, october 2012, p. 47 disponible en la web http://www.ecb.europa.eu en el apartado de *Research & Publications*.

[7] Las características básicas de las cadenas de bloques de carácter público son las que siguen: es «pública» al ser en código abierto de modo que permite que cualquiera pueda descargar una copia y acceder a ella; es «de confianza» porque los sistemas matemáticos de encriptación hacen muy difícil una modificación unilateral de la cadena existente, oponiéndose al consenso; y es «desintermediada» porque no hay una única entidad que controle o manipule la cadena (cfr. FAIRFIELD, «Smart contract, bitcoin, bots

Según se advierte, el carácter descentralizado de la base de datos es lo que permite que no exista un tercero constituido en autoridad que vele por la exactitud y conservación de los registros. No resulta necesario pues son los propios miembros de la cadena los que efectúan tal tarea. Los nodos que forman parte de ella son quienes realizan las verificaciones informáticas precisas para agregar nuevos datos –nuevos «bloques»–, y, cuando estos se añaden, automáticamente se replican en todos los ordenadores de la cadena[8].

---

and consumer protection», *71 Washington and Lee Law Review Online* 35, September, 2014, pp. 36-37 y FARMER, Jr., «Speculative Tech: The Bitcoin Legal Quagmire and the Need for Legal Innovation», *9 Journal of Business & Technology Law* 85, 2014, pp. 89-90). Por otra parte, BUTERIN, «The meaning of decentralization», 6 de febrero de 2017, https://bit.ly/2tEUYyT, alude a tres dimensiones de la descentralización: arquitectónica o de estructura –nodos que están funcionando–, política –cuántos controlan tales nodos– y lógica –si la interfaz y la estructura de datos que sostiene la red es monolítica o multiforme–.

[8] Los nodos que participan en la cadena y que operan «por consenso» son la «autoridad central» que protege el sistema pues no es posible que personas que no se conocen entre sí acuerden en un tiempo breve realizar una acción fraudulenta o que manipule el contenido de la cadena de bloques. En otras palabras: «no hace falta ninguna autoridad ni tercero de confianza cuando la estadística, el cálculo de probabilidades, juega abrumadoramente a favor de la fiabilidad del registro» (GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 41; sobre el difícil ataque a la cadena de bloques, vid. *ídem*, pp. 97-99). De todas maneras, es preciso señalar que cuando ese «consenso» se rompe se debilita el sistema. Son los denominados «*forks*» que originan un desdoblamiento de la cadena. Ello puede deberse bien a discrepancias sobre el software a utilizar, bien porque se escriben dos bloques al mismo nivel con poco tiempo de diferencia y con contenidos contradictorios, bien a otras razones. En el supuesto de los dos bloques «incompatibles», la cadena se sigue construyendo sobre el que se añadió primero y las operaciones pendientes de la cadena más corta se reagrupan e incorporan en los nuevos bloques de la cadena –ahora– más larga. La cadena corta no se valida y se desestima. Finalmente, es preciso hacer dos matizaciones. En primer lugar, aunque en el texto nos referimos en general a los nodos o a los ordenadores de la cadena, no todos tienen la misma función: unos solo emiten transacciones –*broadcast nodes*–, otros las reciben y las retransmiten a la vez que pueden verificar las firmas y los saldos de que se dispone en las transacciones –*relay nodes*–; y finalmente, otros emiten, transmiten y «minan» transacciones –*mining nodes*–. En segundo lugar, aun cuando, en teoría y de acuerdo con la idea inicial de NAKAMOTO, cualquiera puede ser «minero», en la práctica no es tan así. La inversión en material que se necesita, así como el gasto energético, hace que no sea tan abierto el sistema. A consecuencia de lo anterior, actualmente existen «granjas de mineros» o «pozos de minería» –*mining pools*– a los que un usuario particular puede *ceder* su poder de computación. Los *mining pools* son conjuntos muy numerosos de máquinas con hardware y software específico para desarrollar la labor de minería y, que, entre todas, aumentan el poder de computación para «cerrar bloques», repartiéndose entre todos los participantes las ganancias que por ello se obtengan (un *mining pool* puede verse en https://es.minergate.com/). Cabe decir entonces que la labor de «minería» se ha «profesionalizado» y se ha concentrado en zonas del globo donde la energía resulta más barata (China, Malasia, Georgia, etc.). Buena prueba de ello es la concentración de las acciones de minado de bloques en grupos de mineros localizados. La consecuencia que se deriva de tal realidad es que, por lo menos el *sistema Bitcoin*, no es tan descentralizado como inicialmente se pretendía, pues no todo el mundo puede minar y las mejoras del software del sistema han de ser aprobadas y aplicadas de hecho por tales mineros (vid., en tal sentido, la información sobre «descentralización» de las cadenas de bloques que se aporta en https://arewedecentralizedyet.com). En cierta medida, depende de ellos tanto la permanencia del sistema –¿qué sucederá cuando el beneficio que reciben por minar sea muy pequeño y su «recompensa» venga determinada por las comisiones de los usuarios? – como su seguridad –al no estar bien distribuida

En definitiva, las «cadenas de bloques» consisten en bases de datos únicas y descentralizadas que permiten el intercambio entre sujetos de bienes o cosas de valor –dinero, títulos, derechos, etc., pero «tokenizados»– y que gozan de la ventaja de no tener que recurrir a una autoridad superior que vele por su funcionamiento al ser todos los miembros de la cadena los encargados de ello[9]. Utilizan protocolos, se sirven de la tecnología *peer-to-peer* y pueden ser usadas por las inteligencias artificiales (AI), pero las cadenas de bloques no son propiamente protocolos, ni una red P2P ni una inteligencia artificial[10]. Según se afirma, los beneficios que puede proporcionar este nuevo modo de trabajar se advertirán con mayor nitidez cuando se use a gran escala, hasta el punto de que –se ha dicho– todos los ciudadanos la utilizarán en alguna medida y, además, supondrá la supresión de numerosos intermediarios. Con todo, actualmente, el mundo de las DLT sigue estando aún en sus primeros estadios de

---

la capacidad de computación es menos difícil el ataque al 51% de los nodos a fin de alterar la cadena ya «escrita»–. Buen ejemplo de lo primero es la modificación operada en Ethereum en agosto de 2018 que supuso la reducción de la emisión de criptomonedas –y su consecuente revalorización–; decisión en la que los mineros tuvieron notable peso. En relación con lo segundo, baste decir ahora que el del 51% no es el único ataque que puede sufrir una cadena de bloques (*ad ex.* el ataque Vector 76 o ataque de una confirmación, el ataque FINNEY) y que, en la actualidad, se prueban otros algoritmos de consenso que aumenten la seguridad (p. ej. el llamado «independent observer node» propuesto por BUTERIN sobre la base de uno elaborado por LESLIE LAMPORT en 1982). En parte por ello, han ido surgiendo voces críticas sobre el pretendido carácter «descentralizado» de las cadenas de bloques. A modo de ejemplo, vid. SCHNEIER, «There's no good reason to trust blockchain technology», 6 de febrero de 2019, https://bit.ly/2WKlRy6.

[9] Tras una época denominada como *Internet de la información*, las cadenas de bloques han abierto una etapa denominada como *Internet del valor*: la red se usa para transferir valor. Tal y como afirma BRIDGERS («Will workplaces be going off the rails on the blockchain? », *20 num. 11 Journal of Internet Law* 3, May, 2017, p. 3): «blockchain technology allows people to exchange things of value with one another without the trusted middlemen we normally rely on to authenticate transactions, such as governments, banks, or even ride-sharing platforms. It allows us to authenticate and exchange assets, such as virtual currency, intellectual property, titles, credentials, resumes, contracts, and personal data, on a decentralized virtual ledger». Según hemos mencionado, dos de las innovaciones más notables de la cadena de bloques son su teórica habilidad para efectuar transmisiones de propiedad directamente –*peer to peer*– sin necesidad de intermediario de confianza, así como para conocer en tiempo real qué es de quien –a salvo lo que luego se dirá respecto del carácter «pseudónimo» de la cadena de bloques– (O'SHIELDS, «Smart contracts. Legal agreements for the blockchain», 21 *North Carolina Banking Institute* 177, March, 2017, p. 181 y FAIRFIELD, «Smart contract, bitcoin, bots and consumer protection», *cit.*, pp. 40-41). En efecto, al conocerse todo el contenido de la cadena, todas las operaciones y criptoactivos son trazables. Por otra parte, existe un sistema multifirma para dirimir los conflictos relativos a la titularidad de un valor o la validez de una transacción. El problema reside en que quien, por ejemplo, se vea privado de la titularidad de una criptomoneda por medio de este sistema de resolución de conflictos no tendrá nadie a quien reclamar, al no existir una autoridad o ente central responsable; aspecto sobre el que volveremos.

[10] En efecto, la cadena de bloques incorpora protocolos y la tecnología P2P en ciertos aspectos, pero no se reduce a ella pues proporciona un método más descentralizado, seguro y eficiente. Asimismo, en el futuro puede incorporar en sus operaciones AI –área de la informática centrada en la habilidad del software para «aprender» sin supervisión humana: «*machine learning*»– pero seguirá siendo algo diferente de ellas.

desarrollo, y, por eso, el ciudadano medio no percibe todavía en la vida diaria las ventajas que puede reportar y quizá son más notorias las dificultades que presenta[11].

## 3. EL FUNCIONAMIENTO DE LA CADENA DE BLOQUES

Como este artículo no es de índole tecnológica, una vez expuesto el concepto de la cadena de bloques únicamente haremos una breve referencia a los conceptos básicos necesarios para entender su funcionamiento técnico sobre la base de cómo opera la cadena de carácter público denominada *Blockchain* –como se ha dicho, buena parte de lo que aquí se dirá resulta de aplicación a las cadenas de bloques en general–. Ello puede ayudar a contextualizar los retos y consecuencias que tiene esta nueva metodología en el ámbito jurídico, y, de manera concreta, los que suscita en relación con los «contratos inteligentes». En particular, aludiremos a tres conceptos nucleares: las claves criptográficas, el algoritmo de resumen o *hash* y la prueba de trabajo. Como se advierte, en las cadenas de bloques las matemáticas son esenciales, pues se necesitan para los algoritmos utilizados tanto en relación a las claves de encriptación asimétrica como a los *hashes*. Es más, por así decir, la seguridad del sistema reposa en las matemáticas[12].

En relación con el primer concepto, cada uno de los usuarios de la red tiene dos claves criptográficas distintas, únicas y conectadas entre sí, cuya finalidad es «autenticar» el contenido del mensaje encriptado: determinar que el mensaje proviene de una fuente

[11] Respecto de los beneficios que proporcionarán las DLT cuando se generalicen a gran escala –o al menos, las plataformas sean capaces de comunicarse entre sí– vid. O'SHIELDS («Smart contracts. Legal agreements for the blockchain», *cit.*, p. 183) que, en concreto, lo refiere al ámbito financiero. De otra parte, afirmando que en el futuro todo trabajador usará o interactuará con la tecnología de la cadena de bloques vid. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 3; y, más recientemente, MARIYA GABRIEL, *Commissioner for Digital Economy and Society*, con ocasión de la firma en el mes de abril de 2018 de la Declaración de 22 países de la UE para el establecimiento de un «*European Blockchain Partnership*», señaló que «in the future, all public services will use blockchain technology». Con el referido acuerdo se busca una amplia cooperación en el intercambio de conocimiento y experiencia en el ámbito técnico y regulatorio para la creación de aplicaciones en una «*blockchain europea*» a través del *Digital Single Market*, que beneficien tanto al sector público como al privado. Y en relación a eliminación de la intermediación vid. KEMP, «Legal Aspects of Artificial Intelligence», *cit.*, nº 19. Por otra parte, en relación a los inconvenientes, baste mencionar aquí el crítico escrito de STINCHCOMBE, «Ten years in, nobody has come up with a use for blockchain», 22 de diciembre de 2017, https://bit.ly/2zqiRKj, donde analiza las promesas hechas y las ventajas que habían de proporcionar las cadenas de bloques y las compara con su desarrollo actual en ámbitos como los micropagos, la banca, la innecesaria supervisión estatal, etc. A lo que parece, el problema de fondo no es la idea en sí misma, sino las dificultades que suscita su implementación. Sobre todas estas cuestiones, vid., recientemente, VV AA, *Criptoderecho. La regulación de Blockchain* –dir. GARCÍA MEXÍA–, La Ley-Wolters Kluwer, Madrid. 2018.

[12] Cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 64. Un resumen del funcionamiento de la cadena de bloques *Blockchain* se recoge en ANGUIANO, «*Blockchain*: fundamentos y perspectiva jurídica. De la confianza al consenso», *Diario La Ley*, nº 18, 16 de mayo de 2018.

auténtica. En este sistema –denominado «de doble clave» o «*public key infrastructure*»–, las claves tienen funciones diversas –una encripta el mensaje y otra lo desencripta– y el conocimiento de una no permite deducir cuál sea la otra. De esta manera, puede darse a conocer una de ellas –la llamada clave «pública»–, mientras que la otra se mantiene como «privada», conociéndola solo su titular[13]. Las características apuntadas y el enlazamiento que existe entre las claves permiten determinar la autenticidad del mensaje enviado si, al aplicarle una determinada clave «pública», se desencripta: significará que el mensaje ha sido encriptado con la clave «privada» correlativa a la clave «pública» utilizada y facilitada por su titular[14].

En segundo lugar, con el término «*hash*» –o algoritmo de resumen– se alude a una secuencia alfanumérica hexadecimal *única* que es el resultado de aplicar un algoritmo a un archivo[15]. Como ese *hash* es único y se corresponde solamente con el archivo sobre el que se haya aplicado el algoritmo, servirá para determinar si se ha manipulado o no: si al aplicar el algoritmo al referido archivo «devuelve» una secuencia diversa de la inicial significará que se ha modificado el archivo, por ínfima que sea tal alteración; la devolución de la misma secuencia será prueba de la no manipulación del archivo. Junto con ello, otra característica del *hash* es que es unidireccional: por sí mismo no proporciona información sobre el contenido del archivo sobre el que se ha aplicado el algoritmo, pues no cabe reconstruir tal contenido a partir del *hash*. Así, el *hash*

[13] En la cadena de bloques *Blockchain*, la «dirección» *Bitcoin* de un usuario es el resultado de aplicar un algoritmo a su clave pública –operación que se denomina *hashear* y que en breve se explicará– y ello es lo que se incluye en las transacciones. La clave pública es una cadena alfanumérica de 26 a 35 caracteres.

[14] En lo que ahora interesa, el carácter descentralizado de la cadena de bloques que soporta los *bitcoins*, supone que no hay una autoridad superior central que atribuya las claves criptográficas mencionadas en el texto y sea responsable de la monitorización o mantenimiento de un registro único con las de todos los usuarios: se atribuyen de manera descentralizada y no existe el indicado registro central. Ello es así, porque lo relevante en dicha cadena es que las transferencias de activos –de *bitcoins*– provengan de quien dice ser su titular –cuya autenticidad, como hemos señalado, se prueba por medio de la aplicación de la clave «pública» que desencripta lo encriptado por la «privada» correlativa– y no la identidad personal real del sujeto titular de las claves (cfr., sobre este aspecto, GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 67 quien señala que *bitcoin* –de acuerdo con la finalidad buscada originariamente– pretende ser solamente dinero «efectivo» y por ello no resulta relevante tal identidad del sujeto. La firma, en el *sistema Bitcoin*, no se utiliza, por tanto, como «un medio de imputación jurídica de una declaración negocial a una concreta persona física o jurídica»). Un problema derivado de que en el *sistema Bitcoin* lo importante sea la autenticidad del mensaje y que se efectúe la transacción pretendida, es que desde un punto de vista jurídico no se examinan los requisitos comúnmente exigidos por el ordenamiento jurídico para la validez de una transacción, ni se incluye el documento que le sirve de fundamento, lo que permite que se paguen deudas no existentes o que se efectúen pagos por el cumplimiento o ejecución de negocios ilegales.

[15] La cadena de bloques *Blockchain* usa, de los existentes, algoritmos SHA-256 para la función del *hashing*.

únicamente es útil –y no es poco– para determinar si se ha producido o no una alteración del contenido del archivo sobre el que se aplicó el algoritmo[16].

El tercer concepto aludido –y que une los dos anteriores– es la *prueba de trabajo* (*Proof of Work*, PoW). Los mensajes o la información a incluir en la cadena de bloques se elaboran utilizando las claves y el algoritmo señalado[17]. Una vez formado el bloque a cerrar con la información de que en cada caso se trate, para proceder al «cierre» e incorporarlo a la cadena existente, es preciso averiguar por medio de pruebas de computación de carácter no determinista el llamado «*nonce*» –*number used only once*– . Este dato numérico, añadido a la información contenida en el bloque, hace que el *hash* resultante de todo el bloque tenga la configuración determinada por el sistema –

[16] Como la función del *hash* es verificar la integridad de un archivo –detectar si ha sido modificado o no–, y no vale para guardar información ni asegurar su procedencia, no impide, por tanto, que el archivo sea materialmente alterado; lo que sí permite es tal detección sin posibilidad de error. Esta función de *integridad* presupone que se tenga «constancia confiable» de cuál era el *hash* correspondiente al archivo original –aspecto que viene facilitado por el «sellado de tiempo» de la cadena de bloques y su carácter inmutable– así como exige que se conserve el documento original. De lo contrario, sería indiferente que los posteriores cotejos den positivo o negativo pues no habría con que confrontarlo (cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., 76).

[17] La *Proof of Work* (*PoW*) que se explica en el texto, no es el único sistema de consenso para el funcionamiento de las cadenas –existen otros muchos como, por ejemplo, la *Proof of Stake* (*PoS*), la *Proof of Burn* (PoB) o la *Proof of Authority* (*PoA*)– al igual que también las hay sin «mineros» ni recompensas, siendo los incentivos para el cierre de bloques de otro tipo y no necesariamente económicos. En cada bloque, además de otros datos (vid. nota n.º 19), se contiene un conjunto de transferencias. Cada mensaje de transferencia de *bitcoins* tiene los siguientes elementos: de una parte, el *hash* de una previa transferencia de la que resulta un saldo disponible a favor del receptor de aquélla –y que ahora es el transferente–, así como la firma electrónica realizada con la clave privada del entonces receptor y ahora transferente y su clave pública; y de otra parte, los *bitcoins* a transferir y la *dirección Bitcoin* del nuevo receptor –que, como dijimos, es el resultado de *hashear* su clave pública (cfr. nota n.º 13)–. Respecto de todo este contenido que conforma el mensaje de una concreta y específica transacción se calcula nuevamente su *hash*, y se incluye en el encabezamiento del bloque. Esta operación permite identificar esa específica transferencia que se realiza, que, como se advierte, sirve para probar que el ahora transferente de *bitcoins* puede disponer de ellos, al tener, al menos, ese saldo disponible a su favor y no estar gastado (sobre la exigencia de *Blockchain* de gastar todos los *bitcoins* de que se dispone cada vez que se efectúa una transferencia, vid. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., pp. 55 y 84). El destinatario del mensaje lo recibirá en poco tiempo –como veremos, cuestión distinta es que tal recepción signifique que ya se haya incluido como parte de un bloque y se haya añadido a la cadena– y habrá de verificar, en primer lugar, que la clave privada con la que se encriptó el mensaje de transferencia de *bitcoins* es la correlativa a la clave pública que se le ha comunicado –se verifica si con esta se «desencripta» el mensaje–; y, en segundo lugar, que la dirección *Bitcoin* del transferente corresponde con su clave pública *hasheada*. O más correctamente, que la dirección *Bitcoin* del beneficiario de la transferencia anterior coincide con el *hash* de la clave pública del entonces beneficiario, y ahora transferente. Una explicación detallada de este procedimiento se contiene en GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 74 y ss.

un *output* específico coincidente con el establecido–, de modo que se pueda «engarzar» a los bloques ya existentes[18].

La averiguación del *nonce* que permite «cerrar» el «bloque» se comunica a otros miembros de la cadena quienes de manera automática realizan rápidas operaciones de verificación: que el *hash* resultante del bloque a cerrar coincide con el *output* establecido por el sistema, que no hay transacciones ilegales –nadie gasta o transfiere activos que no tiene–, que las firmas electrónicas incluidas en el mensaje son auténticas y que la cabecera del bloque a añadir coincide con el *hash* del anterior bloque, garantizando así su engarce en la cadena, al modo de un «tracto sucesivo registral» pero de «carácter informático»[19]. Comprobados esos extremos, se añade el

[18] Tomando como *input* el contenido del bloque y el *nonce*, efectuando la función de *hash* a todo el bloque a añadir se ha de producir un *output* de un tamaño determinado: «a run of leading zeros» (https://en.bitcoin.it/wiki/Nonce). El número de ceros que debe estar en el inicio del *hash* resultante es el previsto por el sistema para que se pueda cerrar un bloque cada diez minutos. En caso de que por la potencia de computación se redujese o aumentase tal cadencia de tiempo, el sistema incrementaría o reduciría el número de ceros al inicio del *output* –lo que aumenta o disminuye la dificultad de hallar el *nonce*– para mantener ese tiempo estimado de diez minutos. De todas maneras, en la actualidad se están desarrollando algunas soluciones que permitan transacciones «inmediatas» –p. ej. Raiden (https://raiden.network)–.

[19] En efecto, uno de los extremos que se verifica es que el ahora transferente recibió por una transferencia anterior y tiene a su disposición los *bitcoins* que pretende transferir; que no los ha «gastado». Así las cosas, el contenido de cada bloque a incluir se compone de: el *hash* del bloque anterior, las transacciones que se hayan recopilado y validado –de entre ellas, la primera es la transferencia desde el sistema al que cierra el bloque con su «recompensa»– y el *nonce*. De todo este bloque se calcula su *hash* que será el que identifique al bloque y lo que se incluya en la cadena –para su obtención, las transacciones se agrupan por parejas y se *hashean*, y luego los *hashes* resultantes también se van agrupando por parejas pues así se simplifica la operación; sistema conocido como «árbol de Merkle»–. El *hash* identificador del bloque es el que se incluirá en el bloque siguiente, garantizando el engarce. Por ello, cada vez que se añade un bloque se añade una «nueva autenticación de todo el contenido anterior de la cadena y, por tanto, se incrementa la seguridad de todo el registro» (GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 85). De otra parte, ha de señalarse que el *nonce* que tratan de obtener quienes pretenden cerrar el bloque mediante la *prueba de trabajo* a fin de obtener un *output* determinado –que comience con un número preciso de ceros– es siempre diferente. En efecto, bien porque las transacciones de los usuarios que se incluyen en el bloque sean distintas –los transferentes las comunican dentro del sistema pero pueden no llegar al mismo tiempo a todos los nodos–, bien por el sencillo hecho de que la primera transferencia siempre es a favor del que pretende cerrar el bloque –y todos los que lo intentan son diversos–, el «número de un solo uso» que, en unión al resto del contenido del bloque, debe dar lugar a un *output* determinado es necesariamente distinto. A ello ha de añadirse que el modo de calcular el *nonce* es a base de prueba-error; dado el carácter unidireccional del *hash* no hay un cálculo que de manera automática permita averiguar el *nonce*. Característica que pone a todos los que pretenden añadir el bloque en situación de igualdad pues todos han de buscar *su nonce* a base de prueba-error; introduce la igualdad y aleatoriedad del sistema, aunque mitigada por lo que se señala en la nota n.º 8. Otra cuestión más que ha de tenerse en cuenta es que los que se van encadenando en la cadena y sobre los que existe un sellado de tiempo confiable son los bloques –en concreto, el *hash* de cada bloque–. Y es que, como se ha dicho, si el bloque de cada minero no necesariamente contiene las mismas transacciones que el de otro, cabe que una que se haya recibido con anterioridad se incluya en un bloque que se añade a la cadena con posterioridad a otra que, habiéndose emitido después, se

bloque. Una vez incorporado –en sentido técnico, solo se incorpora el *hash* resultante del bloque–, automáticamente se replica en todos los nodos de la cadena –constando el momento preciso de la incorporación–, constituyendo, así, el mejor sistema de copias de seguridad –una por cada nodo– lo que impide su modificación[20]. De esta manera, todos los usuarios de la cadena tienen en todo momento un registro completo y actualizado de todos los bloques –en el *sistema Bitcoin* indicándose quién transfirió qué a quién–, y, en consecuencia, pueden conocer todas las transacciones anteriores desde el inicio de la cadena y sus *hashes*[21]. Pueden añadir nuevos bloques al final de la cadena, pero no modificar los anteriores, pues, a continuación de dicho bloque, se han ido añadiendo otros «encadenados» a él, de manera que la incorporación de cada bloque ha ido aumentando la seguridad de la cadena[22].

Así las cosas, ha de retenerse que lo único que figura en la cadena son los *hashes* de los bloques, que, al «congelarse» por su introducción en ella, prueban la existencia de las transacciones que contenían. Este orden cronológico de bloques y la imposibilidad de

incluyó en un bloque cuyo *nonce* se averiguó antes. O, en otros términos: no se respeta de manera rigurosa el principio de prioridad en las transacciones desde el momento en que su inclusión depende del descubrimiento de un número aleatorio.

[20] Todo registro en la cadena de bloques produce dos efectos. De una parte, «se fija en el documento un sello electrónico que deja constancia de su existencia, con la configuración que tenga, en un día y hora determinado». Y, de otra, «en la cadena de bloques se almacena, no el documento en sí mismo sino una especie de confirmación de ese sello electrónico que permite cotejar su integridad» (LLOPIS BENLLOCH, «*Blockchain* y profesión notarial», https://bit.ly/2RpHa8k). Sentado lo anterior, en las páginas que siguen aludiremos de manera casi indistinta y no siempre técnica a «transacciones», «datos», «registros» u «operaciones» que se incluyen en la cadena de bloques. El uso del término «transacción» se debe a que fundamentalmente la finalidad principal del *sistema Bitcoin* es crear un modo de pago de carácter alternativo al vigente (actualmente, hay otras cadenas de bloques –p. ej. Ethereum– que permiten más funcionalidades que los meros «pagos» o «transacciones»). Señalamos que en ocasiones se usa de manera no técnica pues con tales términos no se quiere aludir siempre a contrato o negocio jurídico sino a la introducción o transferencia de datos en un registro que bien puede referirse a un pago, a una transferencia de activos, a la inserción de un «contrato inteligente», a la determinación de una de sus variables, u otras opciones –aun cuando lo que realmente se incluye en la cadena de bloques es el *hash* de dicha información– (en sentido parecido, vid. IBAÑEZ JIMÉNEZ, *Derecho de blockchain y de la tecnología de registros distribuido*, cit., pp. 43, 44 y 89). Así las cosas, el cotejo es el que permite detectar la modificación a que hemos aludido con anterioridad: cuando la correlación entre la confirmación en la cadena de bloques y el sello emita un cotejo negativo será señal de que el archivo original ha sido modificado; en caso contrario, se sabrá que no ha sido alterado, probando que «este contenido existía desde la fecha en que se incorporó a la cadena de bloques» (LLOPIS BENLLOCH, «*Blockchain* y profesión notarial», *cit.*).

[21] Como se indica en el texto, todos los usuarios del sistema tienen acceso a todos los datos, pueden monitorear su historia y asegurarse de la confianza de la cadena (cfr. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 3).

[22] En efecto, los bloques de «transacciones» registradas también se enlazan entre sí, formando «una cadena de seguridad creciente», de manera que, si se manipulase una sola transacción ya incluida en un bloque, no sólo se alteraría el *hash* de ese bloque, sino el de todos los bloques posteriores de la cadena. De esta manera, al introducirse los bloques con un protocolo común y de manera encadenada por medio del *hash*, se respeta la línea temporal (cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 85).

modificarlos permite también evitar un doble gasto o doble pago –que alguien disponga doblemente del mismo número de criptoactivos–: la tarea de llevar la contabilidad de manera ordenada y sistemática que efectúa una entidad financiera a fin de evitar que se disponga de más de lo que se tiene, se consigue en la cadena de bloques, sin la intervención de intermediario alguno, por medio del engarce ordenado y fechado de los bloques y la posibilidad de identificar de manera única cada una de las transacciones que para incorporar a un bloque han sido verificadas[23].

En el *sistema Bitcoin* los usuarios que realizan las pruebas matemáticas para dar con el *nonce* que permita añadir bloques son los llamados «mineros»: como en una «mina de oro», con su *trabajo* de añadir bloques descubren «nuevo valor» que añaden al existente y, por tal tarea, reciben una recompensa en la criptomoneda denominada *bitcoin*[24]. Aun cuando pueda haber muchas personas tratando de descubrir el *nonce* de manera simultánea, solo una será la que lo logre y la que, en consecuencia, añada el bloque a la cadena y reciba la «recompensa» establecida. En dicho momento el sistema genera nuevas criptomonedas a favor del minero, de manera que cada vez que se cierra un bloque se pone más cantidad de monedas en circulación; se añade más valor a la cadena. Las criptomonedas se pueden conseguir entonces de manera originaria –por la labor de minado– o derivativa –por medio de una adquisición o intercambio con alguien que las tenga–[25].

## 4. VENTAJAS E INCONVENIENTES DE LA CADENA DE BLOQUES

Visto el concepto y funcionamiento de las cadenas de bloques, se advierte que es «un nuevo modo de hacer» que cuenta con variadas ventajas en el tráfico jurídico y

[23] Cfr. MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit*. El inventor de *Blockchain* –SATOSHI NAKAMOTO– ya previó el riesgo de doble pago y la solución que propuso consistía en el conocimiento de todas las transacciones previas en que se ha visto envuelta la moneda de que se trate (NAKAMOTO, S., «Bitcoin: A Peer-to-Peer Electronic Cash System», https://bitcoin.org/bitcoin.pdf).

[24] El incremento del número de criptomonedas en el sistema tiene, lógicamente, un efecto inflacionario pues aumenta la masa dineraria total, pero sin que se corresponda con el incremento de riqueza real de una economía (cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 92). Por ello, el *sistema Bitcoin* prevé una reducción paulatina del importe de las recompensas, que será sustituido por comisiones –*fees*– una vez se llegue a la cantidad prevista por NAKAMOTO de 21 millones de *bitcoins* en circulación. Nótese que, entonces, el sistema que intentó eliminar intermediarios y sus costes, lo que finalmente realiza es sustituir unos por otros; eso sí, las comisiones para el minado de bloques son –y previsiblemente serán– menores que las bancarias. Actualmente, el pago de una *fee* no es obligatorio, pero, si se hace voluntariamente se le concede «prioridad» a la verificación de esa transacción. En cualquier caso, la recompensa no la reciben los mineros justo tras añadir el bloque: hay un período de seguridad consistente en un determinado número de bloques que han de añadirse, para evitar las dificultades que generan los *forks* y un potencial doble uso de las criptomonedas.

[25] Cfr. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 51.

económico. Ahora bien, no son pocos los inconvenientes a que ha de hacer frente y dar respuesta. Veámoslos de manera somera.

De entrada, cabe apuntar que las principales ventajas de la cadena de bloques se derivan de que se trate de un registro inmutable que se va incrementando ordenadamente en el tiempo. Por ello, en teoría cabe utilizar la DLT con una «función registral» sin necesidad de que exista una autoridad superior centralizada que realice tal operación[26]; aspecto sobre el que luego volveremos detenidamente. Podría constituir, entonces, un modo eficiente para probar propiedades reales o personales entre particulares, y, servir, asimismo, como instrumento para poder transferir tales propiedades –utilizando, por ejemplo, los *smart contracts*–[27].

Este carácter inmodificable a que aludimos se erige también en el principal apoyo para la utilización de las cadenas de bloques en el ámbito financiero[28], en el de los seguros –reaseguros, seguros de salud o las reclamaciones contra las compañías[29]– o en el de los

[26] Así lo apunta JOHNSON («Planning the future, Blockchain Technology and the Insurance Industry», 12 num. 4 *In-House Defense Quarterly* 73, fall, 2017, p. 6) cuando afirma que «*Blockchain* technology also provides a manner in which we can preserve ownership rights. *Blockchain*s can serve as public registries for deeds, titles, or licenses». En definitiva, es una herramienta que puede servir para probar la propiedad y almacenar registros sin estar bajo el control o la monitorización gubernamental. De todos modos, no se ha de olvidar lo señalado en la nota n.º 4 sobre la legitimación jurídica que se le atribuya a la *tokenización*. Así, aunque fundamentalmente sean las compañías financieras las que más han invertido en desarrollar cadenas de bloques para el «stock trading», en teoría las DLT resultan eficientes y transparentes no solo en ese ámbito sino también para los registros de propiedades reales o personales, así como para patentar y distribuir la propiedad (cfr. MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit.*).

[27] «A corollary to *blockchain* as a ledger of property rights is that it can also serve as the platform for the transfer, from one party to another, of such property rights» (JOHNSON, «Planning the future…», *cit.*). Vid, en el mismo sentido, FAIRFIELD, «Smart contract, bitcoin, bots and consumer protection», *cit.*, p. 38. De todas maneras, en el apartado 5.3 al analizar la función de registro de las cadenas de bloques se apuntan los inconvenientes –a día de hoy, insalvables– que empañan la visión optimista señalada en el texto.

[28] Según apunta ARRUÑADA («Blockchain's Struggle to Deliver Impersonal Exchange», *cit.*, pp. 77-78), la razón por la que parece que *blockchain* ganará fuerza en el ámbito financiero es debido al «role of simplicity and the scope for *ex ante* completion», de manera especial en el ámbito de los pagos y del comercio de derivados. En sentido similar y respecto de la conveniencia de la simplicidad en los *smart contract*, vid. ARRUÑADA, «Limitaciones de *blockchain* en contratos y propiedad», *cit.*, pp. 2470, 2473 y 2474. Sobre el impacto de las cadenas de bloques en la banca vid. DÍEZ GARCÍA y GÓMEZ LARDIES «Banca y *blockchain*, ¿pioneros por necesidad?», en VV AA, *Blockchain: la revolución industrial de internet* –coord. PREUKSCHAT, A.–, Gestión 2000, Barcelona, 2017, pp. 32-42. En esta obra se analiza el impacto de *blockchain* en otros ámbitos: seguros, telecomunicaciones, farmacéutico, juegos *online*, medios de comunicación, sector público, etc. Baste, por tanto, esta remisión general en lugar de efectuar referencias específicas en las siguientes notas. Asimismo, y de lo expuesto hasta ahora se deduce con facilidad que algunos ejemplos de los señalados en el texto solo tendrían sentido en cadenas de bloques privadas.

[29] Como registro inmodificable de datos permitiría contrastar el estado, el contenido y el alcance del riesgo que se asegura sin necesidad de invertir tiempo y dinero en la coordinación y consecución de dicha información, disminuyendo, en consecuencia, el fraude. Igualmente, disponer de toda esa

recursos humanos[30]; aun cuando en teoría pueda utilizarse en otros muchos ámbitos[31]. Así, si la cadena de bloques se configura de modo que permita conservar documentos,

información –con ese carácter no modificable–, en unión con oráculos de confianza facilita la gestión tanto de los reaseguros –por ejemplo, con apoyo en los «contratos inteligentes», de manera que se suscriban los contratos una vez se cumplan las circunstancias predefinidas– como de las eventuales reclamaciones automáticas y pagos (cfr. JOHNSON, «Planning the future…», *cit.*). A modo de ejemplo, AXA está desarrollando seguros en Shanghai en el ámbito de la agricultura utilizando la cadena de bloques y los «contratos inteligentes» para proteger a los productores de los riesgos de la climatología extrema (https://www.digfingroup.com/gre/).

[30] En este ámbito, se ha dicho que las cadenas de bloques transformarán el funcionamiento de los departamentos de recursos humanos pues se podrá gestionar y almacenar de manera segura toda la información sobre los empleados; p. ej., los certificados de su formación, habilidades o competencias, las revisiones salariales o de trabajo, etc. El carácter inmutable de los datos registrados en la cadena de bloques y su «garantía de confianza» –una vez verificados y «subidos» a la cadena, se entiende– eliminan la duda sobre la autenticidad de dicha información. De todas maneras, no parece ser esta la única posibilidad que ofrecen las cadenas de bloques pues, en este ámbito, también pueden valer para que los trabajadores se puedan organizar y firmar sus cartas de representación sin una autoridad central «verificadora»; para que puedan organizar las elecciones de los representantes sindicales, o, en fin, para gestionar o negociar los convenios colectivos. En definitiva, «*blockchain* could give workers even more freedom than they currently enjoy» (cfr. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 4).

[31] A modo de ejemplo, en teoría una cadena de bloques podría usarse para: a) almacenar datos en la nube sin que exista una empresa de la que dependa –p. ej. Dropbox–; b) el voto electrónico (West Virginia –USA–, Zug –Suiza–, Tsukuba –Japón– o Ucrania están desarrollando iniciativas en tal sentido aun cuando no se haya procedido todavía a una votación oficial totalmente *online* usando *blockchain*; asimismo, es oportuno señalar que no son pocas las voces críticas sobre tales posibilidades); c) la toma de decisiones (LASKOWSKI, «A Blockchain-Enabled Participatory Decision Support Framework», VV AA, *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, Springer, Cham, 2017, pp. 329-334); d) la gestión de derechos de autor (cfr. BODÓ, B., GERVAIS, D. y QUINTAIS, J. P., «Blockchain and smart contracts: the missing link in copyright licensing?», *International Journal of Law and Information Technology*, volume 26, Issue 4, 1 December 2018, pp. 311–336, https://doi.org/10.1093/ijlit/eay014 y, en el ámbito musical, vid. *ad ex.* Mycelia, http://myceliaformusic.org); e) diversos servicios públicos –gestión de licencias, servicio de salud, o registro de buques, tal y como se pretende en Dinamarca (https://bit.ly/2sxZMFj)–, u otros. Asimismo, en el Derecho societario, la cadena de bloques parece que permitirá la transferencia inmediata de acciones entre inversores y accionistas –sabiendo qué pertenece a quién en cada momento–, simplificará el sistema de voto haciéndolo más transparente, y posibilitará la automatización del reparto de dividendos, eliminando el margen de error. Elementos todos ellos que más que una mejora del sistema supondrán una transformación radical en el mundo accionarial (cfr. TINIANOW, «Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance», 16 de marzo de 2017, https://bit.ly/2Syeozv). Y, en el sector bancario, la implementación de la cadena de bloques traerá consigo, entre otras ventajas, una mejor comunicación «banco a banco». El desarrollo de protocolos de comunicación entre las diversas entidades, así como la inmediata validación de operaciones permitirá efectuar compensaciones y liquidaciones individuales –reduciéndose los costes–, lo que habrá de traducirse en un mejor servicio al usuario quien, además, se beneficiará de que las transferencias y liquidaciones se realizarán en tiempo real (cfr. SOLEY, «Cómo cambiará *blockchain* tu manera de hacer pagos», *IESEinsight*, nº 35, septiembre-diciembre, 2017, pp. 47-52). Una visión un tanto más crítica –y, a nuestro juicio, más apegada a la realidad práctica– es la que ofrece IVANITSKIY («You Do Not Need Blockchain: Eight Popular Use Cases And Why They Do Not Work», 22 de febrero de 2019, https://bit.ly/2GXjLFC) sobre diversos supuestos donde inicialmente parece que cabría aplicar la cadena de bloques pero que luego no resultan tan adecuados. En su opinión, las transferencias de dinero nativo digital es donde mejor funciona *blockchain*, precisamente por «on-chain transactions, when the system

podrá desarrollar una función de «caja fuerte» que también resulte útil, por ejemplo, en el ámbito notarial[32]. Ahora bien, junto con lo que seguidamente se dirá, la clave de tales usos es que, si finalmente se convierten en realidades, proporcionen las mismas o mayores ventajas que los sistemas actuales, con un mismo o mayor nivel de seguridad, pero a menor coste.

De otra parte, y al margen de lo que se indicará en los siguientes apartados, cabe condensar en tres los principales inconvenientes que plantean las cadenas de bloques de carácter público: pueden contener datos sensibles –lo que se agrava por el mismo carácter inmodificable de la cadena–; su desarrollo todavía es incipiente –y, por ello, su uso demanda mucha potencia de energía, a la vez que genera suspicacia en la población–; y algunas de las criptomonedas que soportan son muy volátiles[33].

De los inconvenientes señalados, el primero de ellos es, en nuestra opinión, el de mayor calado. Si los registros efectuados en las cadenas de bloques no se pueden modificar y hay una copia de todos los realizados desde el inicio de la cadena en cada ordenador, una multitud de usuarios tendrá acceso a información, relativa, por ejemplo, a las transacciones realizadas. Información que puede ser utilizada para cualquier fin[34]. En cualquier caso, se trata de información que las personas o empresas

---

does not need the real world, with all necessary information already being within the blockchain, thus allowing the system to verify data».

[32] Obviamente, para que tenga lugar lo que se apunta en el texto es preciso que la cadena de bloques sea privada y cerrada. De acuerdo con LLOPIS BENLLOCH («*Blockchain* y profesión notarial», *cit.*) «otro uso podría ser el dar garantías de inalterabilidad a la circulación de las copias electrónicas, si ésta circulara fuera del entorno cerrado y seguro de SIGNO». Sobre el creciente papel que pueden tener las cadenas de bloques en la labor de notarización y de archivo vid., ARRUÑADA, «Blockchain's Struggle to Deliver Impersonal Exchange», *cit.*, p. 92, y también en «Blockchain in Public Registries: Don't Expect Too Much», *IPRA Cinder International Review*, nº 1, January-June, 2017, p. 9.

[33] A modo de ejemplo, en agosto de 2010 un *bitcoin* valía 0,07 dólares y el 11 de diciembre de 2017 llegó a valer 17.549,67 dólares (https://www.buybitcoinworldwide.com/es/precio/). Otros riesgos de las cadenas de bloques son los que apunta ECHEBARRÍA SÁENZ («Contratos electrónicos autoejecutables…», *cit.*, pp. 86-89): es posible un riesgo sistémico por colapso operacional; no existen mecanismos de contención como los del sistema bancario frente a un eventual hundimiento generalizado de los agentes que operan en la cadena; cabe un riesgo institucional si las autoridades bancarias coordinan un ataque prohibiendo o limitando las operaciones con criptomonedas pues generarían una gran desinversión y el consiguiente colapso; y, los *hard forks* pueden duplicar nominalmente activos sin base real –como en parte ya sucedió en 2017 en *Blockchain* y en 2016 en Ethereum que provocó la generación de una segunda criptomoneda: *bitcoin cash* y *Ethereum classic*–, lo que resta estabilidad y credibilidad al sistema.

[34] «Some disadvantages of a *blockchain* are that every user could have a copy of a single database, accessible to all, with records of every single transaction. Not everyone would like their every stock transaction permanently saved on a freely accessible database. If the database is open to all, that could permit gathering of information for all kinds of purposes (advertising, crime, data mining), the flip side of transparency. A *blockchain* register, however, might be configured to provide more privacy than some public records that are presently completely open» (MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit.* y BELL, «Copyrights, Privacy, And The Blockchain», 42 *Ohio Northern*

pueden considerar «sensibles», lo que les hará reacios a intervenir en cadenas de bloques públicas[35].

Asimismo, la información contenida en una cadena de bloques puede generar problemas legales en el ámbito de la protección de datos a que habrá de dar respuesta. De entre ellos, destacan los siguientes: la determinación de quienes son los responsables del tratamiento –*data controllers*– así como la viabilidad de cumplimiento de las obligaciones que les corresponden, la anonimización de los datos personales, o, en fin, el ejercicio de algunos derechos subjetivos relativos a los datos. Según se advierte de lo hasta ahora expuesto, los problemas de compatibilidad con el Reglamento (UE) 2016/679, de 27 de abril de 2016, cuya entrada en vigor ha tenido lugar el 25 de mayo de 2018, son mayores en las cadenas de bloques públicas que en las de carácter privado y no han sido resueltos de manera definitiva ni por las legislaciones de los diversos países ni por las autoridades comunitarias en protección de datos[36].

Por lo que hace a la determinación de los responsables del tratamiento en las cadenas públicas, no es una cuestión que tenga una respuesta clara. En efecto, no parece que puedan considerarse como tales a los desarrolladores del código que subyace en las cadenas: con frecuencia son voluntarios que no reciben compensación alguna por tal trabajo ni tampoco son los responsables del software *open-source* que ayudan a mantener. Tampoco parece que puedan calificarse como tales a los nodos que validan transacciones pues con tal actuación no determinan el propósito de éstas ni los medios de procesamiento: únicamente cierran bloques para recibir la recompensa establecida. Si lo anterior ocurre respecto de los nodos validadores, igual conclusión ha de inferirse respecto de los usuarios de la cadena que firman y emiten transacciones cuando aportan sus datos personales. Distinta sería la situación si realizasen una actividad

*University Law Review* 439, 2016). De otra parte, incorporar todos los datos en una única base de datos podría ser un incentivo para un riesgo sistémico, en el caso de que, por ejemplo, los mineros se pusiesen de acuerdo para tomar el control de la cadena de bloques; aspecto que, como vimos, no resulta sencillo. Finalmente, ha de apuntarse que actualmente se trabaja en sistemas de «poda» de datos, de modo que no se conserve en todos y cada uno de los nodos toda la información de la cadena.

[35] «*Blockchains* can contain a massive amount of personally identifiable information and other related data»; motivo por el que las empresas han de ser cuidadosas a la hora de decidir si utilizan o no esta tecnología –en cadenas públicas, se entiende– (cfr. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 5).

[36] En tal sentido, el Informe temático sobre «Blockchain and the GDPR» elaborado por THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, 16 de octubre de 2018, disponible en https://www.eublockchainforum.eu/reports, indica que no existen problemas de compatibilidad entre la tecnología en sí misma que analizamos y el Reglamento, sino que las dificultades surgen en relación al uso que se le dé a aquellas (p. 4 y 16). Los usos y las aplicaciones que utilicen la referida tecnología serán lo que resulten acordes o no con el Reglamento.

empresarial en la que proporcionasen datos a la cadena, ya que, en tal caso, sí podrían ser considerados responsables del tratamiento[37].

Por lo que hace al carácter de los datos, baste decir ahora que el Reglamento no se aplica a datos anónimos. Para que puedan considerarse así, es preciso que la operación de «anonimización» sea irreversible de manera que no quepa la reconstrucción de los originales a partir del resultado y se impida que unos en unión con otros permitan identificar a la persona. Cuando no se cumplan todos esos requerimientos, los datos no serán «anónimos» sino «pseudónimos». Por lo que hace a las cadenas públicas –en particular, a *Blockchain*– en ella únicamente figura un número de referencia –un identificador– y no la identidad personal real del sujeto. De todos modos, por diversos medios cabe averiguar cierta información sobre el sujeto –por ejemplo, por las transacciones que realiza, por los patrones de actuación, por medio de las IP utilizadas– ; en este sentido, *Blockchain* no es una cadena «anónima» sino «pseudónima»[38].

[37] Cfr. THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, «Blockchain and the GDPR», cit. pp. 17-18. Considerando como responsables del tratamiento a los nodos y mineros cuando tienen un papel activo y no solo procesan datos, vid., BACON ET ALII, «Blockchain demystified: a technical legal introduction to distributed and centralized ledgers», *Richmond Journal of Law & Technology,* volume 25, issue 1, 2018, pp. 63-72. En cualquier caso, tales autores los consideran como encargados del tratamiento –*data processors*–: «if a blockchain platform is used to process personal data, the users, nodes, and miners of blockchain platforms may be either data controllers, processors, or potentially both. If so, they will need to comply with data protection obligations and may be exposed to substantial penalties for breaches of data protection laws. With open, distributed platforms, even if all parties involved were deemed joint controllers, it is not clear how they would comply with their obligations (such as to establish responsibilities by contract and respond appropriately to the exercise of data subjects' rights)» (*ídem*, p. 105). Finalmente, defendiendo que los usuarios de *blockchain* son responsables del tratamiento en relación a los datos personales que ellos suben a la cadena y encargados del tratamiento al almacenar una copia completa de aquella en su ordenador vid. el nº 8 de la Opinión sobre *blockchain* elaborada por el COMITÉ SOBRE LAS LIBERTADES CIVILES, JUSTICIA Y ASUNTOS INTERNOS del Parlamento Europeo para el Comité de Transacciones Internacionales (2018/2085(INI)) de 15 de noviembre de 2018, disponible en https://bit.ly/2Rxr6RK.

[38] En efecto, «privacy is preserved by the nature of the functioning of the *Blockchain*. The *Blockchain* does not need to know who anybody is» (JOHNSON, «Planning the future…», *cit.*). «On the *Blockchain*, participants can choose to maintain a degree of personal anonymity» (TAPSCOTT & TAPSCOTT, *Blockchain revolution…*, cit., p. 43). La pseudonimización no elimina el carácter «personal» de los datos si, de acuerdo con la jurisprudencia del TJUE, combinados con otros, permiten identificar a la persona (Breyer v. Germany, C 582/14, de 19 de octubre de 2016, nº 31 y 39). Como se indica en el texto, hay diversos métodos para determinar identidades en *Blockchain* (un elenco de ellos se recoge en BACON ET ALII, «Blockchain demystified…», *cit.*, pp. 61-63; y sobre la misma cuestión de la «privacidad» en *blockchain*, vid. STRICK, «Tracing an offshore bank and a dark web service using the blockchain — an OSINT investigation», 6 de septiembre de 2018, https://bit.ly/2Ho0cGN y WALL, «Privacy and Cryptocurrency, Part I: How Private is Bitcoin?», 7 de marzo de 2019, https://bit.ly/2EL7lxX). A fin de evitar tales problemas caben variadas soluciones: almacenar los datos personales en una base encriptada que esté fuera de la red o acudir a las diversas técnicas existentes para generar datos anónimos con los requisitos exigidos por el Reglamento, tal y como está realizando Zcash y su protocolo P4 (Private Periodic Payment Protocol) o como está ensayando la *blockchain* privada Hyperledger Fabric. En tal sentido, vid. el listado

Y, por lo que hace a la posibilidad de ejercicio de algunos derechos subjetivos relativos a los datos, se erige en una dificultad en las cadenas públicas[39]. En lo que ahora interesa, destaca el denominado «derecho al olvido», recogido en el artículo 17 del Reglamento (UE) 2016/679. De acuerdo con dicho precepto, a todo interesado le asiste en las circunstancias que en él se señalan el derecho a «*obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales*»[40]. Aspecto que, según se advierte, choca con varias de las principales características de las cadenas de bloques de carácter público: su carácter inmutable y la inexistencia de una autoridad superior responsable que monitoree la actividad[41]. Como el propio Reglamento no explica qué significa el «borrado», las soluciones que se han propuesto en este contexto son variadas: que los Estados en sus legislaciones excluyan las cadenas de bloques de la aplicación de dicho derecho; que haya cadenas de bloques editables; que se entienda que el *hash* y su carácter unidireccional cumplen con la privacidad; que se mantengan fuera de la cadena de bloques los datos personales; que se encripten los datos con una contraseña y que ésta se elimine cuando se solicite el ejercicio del

incluido en THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, «Blockchain and the GDPR», cit., pp. 19 y ss.

[39] Otras cuestiones relativas a los datos son si hay emisión de consentimiento acorde con el Reglamento cuando el usuario utiliza la cadena de bloques, la dificultad de ejercitar el derecho de acceso si no hay un responsable del tratamiento identificado, la imposibilidad de fijar un plazo de conservación de los datos personales, etc.

[40] En este ámbito, es particularmente interesante la sentencia del Tribunal de Justicia de la Unión Europea sobre el derecho al olvido de 13 de mayo de 2014 (TJCE 2014, 85), Caso Google Spain S.L contra Agencia Española de Protección de Datos (AEPD); y en nuestro país la STS de 15 de octubre de 2015 (RJ 2015, 4132). De acuerdo con el nuevo Reglamento de Protección de Datos de la Unión Europea, entre otras circunstancias que permiten ejercitar el «derecho al olvido», cabe mencionar que: «*a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a, o el artículo 9, apartado 2, letra a, y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1*». A continuación, el apartado segundo del artículo 17 señala las medidas que debe adoptar el responsable del tratamiento de los datos. Y el apartado tercero incluye los supuestos en que no serán de aplicación los dos primeros: por razones de interés público, para ejercer el derecho a la libertad de información, etc.

[41] Sobre que la inmutabilidad es uno de los elementos básicos de las cadenas de bloques y en el que se apoya la confianza que genera cfr. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, pp. 5. y 6. Incidiendo en las dificultades que suscitan las cadenas de bloques públicas en relación con el «derecho al olvido», vid. el nº 9 de la Opinión sobre *blockchain* elaborada por el COMITÉ SOBRE LAS LIBERTADES CIVILES, JUSTICIA Y ASUNTOS INTERNOS del Parlamento Europeo para el Comité de Transacciones Internacionales (2018/2085(INI)) de 15 de noviembre de 2018, disponible en https://bit.ly/2Rxr6RK.

«derecho al olvido», etc.; a nuestro juicio, ninguna parece dar respuesta adecuada al problema[42].

En relación con el segundo inconveniente anteriormente señalado –el carácter incipiente de la tecnología, la demanda de energía y las reticencias del ciudadano medio–, basta apuntar ahora que, con el estado actual de desarrollo de las cadenas de bloques, se precisa mucha energía para realizar las operaciones de averiguación del *nonce* y el consiguiente cerrado de bloques; necesidad que supone una inversión considerable para las empresas que quieran crear una cadena de bloques con características similares y trabajar con esta infraestructura –que, como es conocido, constituye una plataforma adecuada para los *smart contract*–[43]. Además, la existencia de diversas cadenas –cada una con sus características propias– hace que actualmente coexistan varios ecosistemas sin que haya unos estándares y protocolos comunes, lo que dificulta la comunicación entre ellos[44].

[42] En efecto, la exclusión a nivel nacional vulneraría una de las principales finalidades del Reglamento europeo de Protección de Datos, que pretende armonizar las legislaciones nacionales evitando la disparidad normativa y de ámbitos de protección. Por otro lado, las cadenas editables vulneran la esencial inmutabilidad que caracteriza a dicha tecnología y parece exigir una autoridad superior; lo que contraviene el carácter descentralizado. Estudiando algunas de las posibilidades citadas en el texto, vid. FRIDMAN, A., *How to design a GDPR-compliant blockchain*, 23 de mayo de 2018, https://bit.ly/2GON49D; y en España, vid. IBAÑEZ JIMÉNEZ, *Derecho de blockchain y de la tecnología de registros distribuido*, cit., p. 339.

[43] Cfr. JOHNSON, «Planning the future…», *cit.* En este sentido, un informe de junio de 2014 de la National University of Ireland Maynooth indicaba que el consumo de energía que requería el minado de *bitcoin* era comparable al uso de electricidad de toda Irlanda (cfr. KEMP, «Legal Aspects of Artificial Intelligence», *cit.*, nº 19). Evidentemente, tales dificultades técnicas se van resolviendo con el avance de los años, posibilitando la creación de más y mayores cadenas. De otra parte, no dejan de surgir noticias relacionadas con la energía empleada en la «minería», de las que destacamos las siguientes: la intención de China de establecer restricciones en el consumo energético para evitar tener una economía demasiado apoyada en las criptomonedas (https://bit.ly/2CLNz5E); la proposición aprobada en Plattsburgh (New York) por medio de la Local Law P-3 de 2018 –que añade el §270-28-J en el Capítulo 270, Artículo V, del *City Code* de Plattsburgh– con la finalidad de fijar una moratoria para realizar operaciones de minado en esa ciudad, donde la energía es especialmente barata; la aprobación de la ley HB 19 en Wyoming (USA) eximiendo las criptomonedas del Wyoming Money Transmitter Act a fin de atraer a empresas que trabajen con ellas (https://legiscan.com/WY/bill/HB0019/2018); el hecho de que en las cadenas de bloques privadas se comience a usar otros algoritmos de consenso –p. ej. la «prueba de autoridad»– en vez de la «prueba de trabajo» ya que consumen menos energía en el minado (https://bit.ly/2C2NbxQ); y, finalmente, que el abaratamiento de la energía hace que sea menos difícil el ataque al 51% de la cadena de bloques (https://bit.ly/2R5z4lH).

[44] Algunos de los objetivos o tendencias de las cadenas de bloques para 2018 consistía en facilitar la interacción por medio del uso de *sidechains*; vid. WIRDUM, A. v., «Keep an eye out for these bitcoin tech trends in 2018», 2 de enero de 2018, https://bit.ly/2E4xNAp. Con una cadena lateral se puede utilizar el *sistema Bitcoin* y sus ventajas para finalidades diversas a las de la transferencia de *bitcoins* –que, recordemos, es la finalidad originaria de la *Blockchain*–. A modo de ejemplo, para el registro electrónico de ficheros. Otro de los problemas de *Blockchain* que no hemos mencionado en el texto es su escalabilidad o el elevado coste que conlleva el envío de pequeñas cantidades de dinero. Para la

Y finalmente, en lo que atañe a la tercera dificultad apuntada –la volatilidad de algunas criptomonedas– constituye un obstáculo para el uso generalizado por los usuarios, pues, entre otras razones, su valor puede aumentar o disminuir notablemente en breves períodos de tiempo. Para que se generalicen las cadenas de bloques y el uso de las criptomonedas es preciso que exista más estabilidad[45].

## 5. REGULACIÓN LEGAL DE LA CADENA DE BLOQUES Y RETOS JURÍDICOS QUE PLANTEA

### 5.1. *Introducción*

Aun cuando en algunos ordenamientos jurídicos de otras partes del mundo ya se han introducido referencias a las cadenas de bloques, en la realidad jurídica española no existe ninguna mención a ellas a nivel legal[46]. Por tanto, no contamos más que con la

resolución de estos problemas se ha implementado la herramienta *Lightning Network* que permite la tramitación de pagos y micropagos de forma casi instantánea gracias a *smart contracts* que no requieren de la creación de una transacción para cada pago. Esta red utiliza un protocolo como capa secundaria a *Bitcoin*. En parte, ello es debido al problema del tamaño de los bloques: a mayor tamaño se incluyen más transacciones haciendo al sistema competitivo como medio de pago, pero, entre otros, tiene también el problema de que se tarda más en minar, y, consecuentemente, se «desincentiva» tal operación porque se reducen las recompensas para los mineros. Un buen resumen del indicado problema se contiene en GALLEGO FERNÁNDEZ, «Cadenas de bloques y Registros de derechos», *Revista Crítica de Derecho Inmobiliario*, nº 765, enero-febrero, 2018, pp. 115 a 118. Otros mecanismos que actualmente se están usando –por lo menos en Ethereum– para resolver los problemas de escalabilidad son *Plasma* –que supone la creación de «sub-cadenas»–, *Casper* –que es un algoritmo de consenso– y *Sharding*, que conlleva dividir en fragmentos la información. Finalmente, señalando la escalabilidad y la interoperabilidad como dos de los grandes retos de las cadenas de bloques, vid. el reciente Informe temático sobre «Scalability, interoperability and sustainability of blockchains» elaborado por THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, 6 de marzo de 2019, disponible en https://bit.ly/2EZhgQl.

[45] Buena prueba de lo que se indica en el texto son las decisiones de algunos bancos (JPMorgan Chase & Co., Bank of America Corp, Citigroup, Lloyds Bankc, etc.) que han limitado o restringido operaciones crediticias para la adquisición de criptomonedas –en especial, *bitcoins*– pues por su volatilidad genera incertidumbre sobre la devolución de los créditos. Asimismo, son conocidas las noticias relativas a robos de criptomonedas –de los más recientes, los 535 millones de dólares en la criptomoneda NEM–. Aludiendo a la fluctuación de la criptomoneda vid. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 6. Como señala dicho autor, por ejemplo, la volatilidad de la moneda hace que pagar a los trabajadores con *bitcoin* aumente el riesgo de vulnerar lo establecido en los convenios en relación a los salarios y horas extras. Parece más adecuado usar los *bitcoin* como *bonus* y no para el pago del salario base. De todos modos, junto con la fluctuación de la moneda virtual no ha de olvidarse que todavía es algo desconocida y no muy aceptada en los negocios diarios. Por lo que se refiere a España, cabe pactar el abono del salario en criptomonedas *ex artículo* 3.1.c del Estatuto de los Trabajadores; lo que no sería posible es su imposición por el empresario. Y, sobre si se debe aplicar a las criptomonedas la limitación del abono del 30% del salario «en especie» (cfr. art. 26.1 ET), la respuesta ha de ser positiva, salvo que, de acuerdo con la STS de 24 de octubre de 2001 (RJ 2002, 2363) se considere que la existencia de la posibilidad de cambiarla de manera inmediata en dinero, la convierta en salario metálico y no en especie.

[46] Un análisis bastante completo de las diversas estrategias de los legisladores ante la realidad de las cadenas de bloques se contiene en FINCK, «Blockchain regulation», *cit.*, pp. 9-16. En dicho estudio, la autora distingue cinco reacciones y pone ejemplos de países que los aplican: 1) «wait-and-see»: esperar

legislación general para afrontar tal novedad; en lo que ahora importa, y de manera meramente ejemplificativa, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico, la Ley 21/2011, de 26 de junio, de Dinero Electrónico y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (en adelante LSSI, LDE y la LFE)[47].

---

y ver como se desenvuelve esta nueva tecnología y hasta entonces aplicar el ordenamiento vigente, bajo el eslogan «educate, don't regulate»; 2) la aprobación «informal» de guías o criterios –no, por tanto, de normas vinculantes– sobre cómo aplicar el ordenamiento vigente; 3) «sandboxing»: a fin de atraer empresas que utilizan las DLT se aprueba un conjunto de reglas que permite a los innovadores desarrollar sus productos o modelos de negocio en un entorno que de manera temporal les exime de algunas exigencias legales; 4) la aprobación de nueva legislación, con la ventaja de la seguridad que aporta contar con una regulación pero también el potencial inconveniente de ser prematura; y 5) la utilización de las cadenas de bloques por parte de los reguladores para investigar usos que resulten útiles para el Estado. Junto con ello, la citada autora también contiene una serie de principios que han de seguirse en cualquier regulación de las cadenas de bloques que se lleve a cabo (*ídem*, pp. 16-23). Por otra parte, y a modo de ejemplo, en Europa, cabe mencionar la regulación sobre *Blockchain* del Principado de Mónaco (https://bit.ly/2Qi21pz) y las normas sobre DLT o criptomonedas aprobadas en Malta (https://bit.ly/2LqdLoG), o el proyecto de ley de Luxemburgo que permite transmitir *securities* a través de *blockchain* (https://bit.ly/2RjGIIJ). En Estados Unidos señalamos cuatro ejemplos: el Estado de Arizona que ha aprobado el 29 de marzo de 2017 la «Blockchain Bill» (House Bill 2417) modificando la sección §44-7003 de los *Arizona Revised Statutes* para reconocer como firma legal la realizada en *blockchain* (https://bit.ly/2TpyNag); la propuesta de ley introducida en New Hampshire el 20 de febrero de 2019 (NH HB470) que, por ejemplo, permitiría pagar los impuestos con criptomonedas (https://legiscan.com/NH/sponsors/HB470/2019); la propuesta de aplicar el artículo 4.a del *Uniform Commercial Code* al sistema de pagos utilizando *bitcoin* (HUGHES, S. J., y MIDDLEBROOK, S. T., «Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries», 32 *Yale Journal on Regulation*, 495, 2015); o que la *Uniform Law Commission* tenga un Comité trabajando para elaborar una *Uniform Regulation of Virtual Currency Businesses Act* (https://bit.ly/2VssAw3).

[47] En el contexto internacional, tampoco existe una tendencia uniforme respecto del uso o no de la criptomoneda. Así, mientras que Japón ha autorizado el *bitcoin* como medio de pago legal y el Tribunal Supremo de Korea lo ha reconocido como activo y no como divisa, son más numerosos los países que lo prohíben (Bolivia, Ecuador, Islandia, Rusia, etc.). De todos modos, parecen mayoría los Estados que, sin regularlos expresamente ni prohibirlos, optan por equiparar los *bitcoins* a otros activos financieros existentes. A modo de ejemplo, en Estados Unidos, desde el 27 de marzo de 2014 el *Inland Revenue Service* (IRS) los ha clasificado como un negocio de servicios monetarios (MSB) estando presente en los mercados de derivados; Canadá y Australia consideran las transacciones con *bitcoin* como trueques, existiendo obligación de registrar los «intercambios» en el Centro de Análisis de Transacciones Financieras de Canadá o reconociendo su sujeción a los impuestos correspondientes en Australia. De todos modos, en Australia ya en 2015 se propuso considerar las transacciones con criptomonedas como las realizadas con dinero –en lugar de considerarlas activos intangibles–, reconociendo, en consecuencia, su exención a efectos de IVA (*Good and services tax*; *GST*). En la Unión Europea no hay una regulación común, y cada país sigue su propio criterio: en Holanda se consideran transacciones de trueque sin necesidad de una licencia específica; en España hay advertencias de los organismos reguladores y algunas consultas en materia tributaria, que se explican en el apartado 5.5.5 de este artículo. De todos modos, recientemente la Unión Europea ha publicado un informe donde se plantea crear una criptomoneda de curso legal para, aun siendo conscientes de los riesgos que conlleva –por ejemplo, su volatilidad– dar mayor estabilidad al sistema financiero (https://bit.ly/2s3HY4u). Junto con ello, y por lo que se refiere específicamente a las «ofertas iniciales de criptomonedas» en España, resultan de interés los siguientes documentos: a) el Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs) de 8 de febrero de 2018

De la mera inexistencia de una regulación específica de las cadenas de bloques no cabe deducir –como parece lógico– que esta metodología o herramienta no suscite reto jurídico alguno, además de otras cuestiones de ámbito político[48]. Como es de suponer, tarde o temprano, la legislación se adaptará a ella, al igual que ha sucedido con otras herramientas tecnológicas. Sea como fuere, en el presente epígrafe pasaremos revista a algunos de los retos que presentan las cadenas de carácter público –en especial, de *Blockchain*–; en concreto: la falta de dueño, los límites de la función registral que desempeña, algunos aspectos sobre la identidad de los intervinientes y su capacidad para operar en la cadena de bloques, y, finalmente haremos mención a *bitcoin*, la criptomoneda propia de *Blockchain*[49].

### 5.2. *Ausencia de dueño*

Según se ha explicado, una cadena de bloques pública es una base de datos descentralizada que permite operar a sus usuarios sin que exista una autoridad superior que monitoree o controle las transacciones que en ella se realizan. Esta configuración, que goza, sin duda, de ventajas, también presenta, entre otros, un inconveniente importante: al no constituir una empresa, sino –digámoslo así– una red colaborativa, no existe una persona jurídica detrás ni una institución que sea su propietaria, responsable o administradora. En consecuencia, en casos de fallo del sistema, de *hackeo*, de mal funcionamiento de la cadena, de un *fork* que disminuya el valor de las criptomonedas, o, en fin, y entre otros, de la privación de la titularidad de

(https://bit.ly/2G5JBaf); b) las Consideraciones de la CNMV sobre «criptomonedas» e «ICOs» dirigidas a los profesionales del sector financiero de 8 de febrero de 2018 (https://bit.ly/2nTGk2G); c) los comunicados de la Autoridad Europea de Valores y Mercados (ESMA) sobre las «ICOs» relativos a los riesgos para los inversores (https://bit.ly/2pqpOZ2) o con advertencias para los consumidores que pretendan comprar criptomonedas (https://bit.ly/2sjUTSA). Un análisis de las actitudes regulatorias de variados países en relación a las ICO se encuentra en KAAL, «Initial Coin Offerings: the top 25 jurisdictions and their comparative regulatory responses», 3 de febrero de 2018, https://bit.ly/2nM75WG.

[48] Entre otros retos, MCJOHN y MCJOHN sugieren «how to legally characterize *bitcoin* and other *blockchain* technologies and how to regulate it, if at all, or even ban it, has attracted increasing attention. Tax issues have already arisen. Commercial law will likewise need some adaptation» («The Commercial Law of Bitcoin and Blockchain Transactions», *cit.*). De otra parte, como apunta GONZÁLEZ-MENESES (*Entender Blockchain…*, cit., pp. 14-27), *Blockchain* y *bitcoin* han de examinarse desde una triple perspectiva: la tecnológica, la económica y la política. Y es que la creación de un sistema monetario sin intermediarios, así como que el control de una moneda que circula a nivel mundial se realice exclusivamente por una comunidad de usuarios y se base únicamente en la oferta y la demanda, es un aspecto que «entra de lleno en el ámbito de lo político. En último término, no estamos hablando solo de costes, sino de poder» (*ídem*, p. 18); motivo por el cual se da la paradoja –como señala el autor–, de que lo que surgió como contestación al sistema financiero tradicional suscita cada vez un mayor interés por parte de éste (*ídem*, p. 28).

[49] En este aspecto, vid. GONZÁLEZ-MENESES, «La reflexión pendiente sobre *blockchain*», 14 de marzo de 2018, https://bit.ly/2Tos4Ny, que contiene un interesante elenco de cuestiones jurídicas, políticas y económicas que han de plantearse respecto de la cadena de bloques; la mayor parte de ellas se abordan en este texto.

criptoactivos por medio de la resolución de conflictos multifirma, no habrá una entidad a quien reclamar y que deba de hacer frente a la responsabilidad que eventualmente pudiese surgir, sea civil, penal o de otro tipo[50]. Este hecho invitará, como parece sensato, a que los potenciales intervinientes –especialmente, cuando pretendan invertir gran cantidad de tiempo o dinero– deliberen de manera detenida la conveniencia de participar o no en cadenas de bloques de carácter público.

### 5.3. *La función de registro: límites y características*

Una segunda cuestión que cabe abordar ahora es la que se refiere a los límites y características propias de la función de registro que realiza la cadena de bloques. Aunque el carácter inmutable de los datos contenidos en ella la convierten en un mecanismo seguro para registrar transacciones tiene limitaciones. Entre otras, cabe apuntar: que la función de registro no es totalmente abierta, pues, de hecho, hay restricciones en el acceso; que la inclusión de documentos no es una característica habitual de las cadenas de bloques –e incluso no buscada en algunas de ellas, en atención a su carácter público y su finalidad–[51]; y que tal registro únicamente incluye un «sellado de tiempo».

Aun cuando la pretensión fundamental de una cadena de bloques sea constituir una herramienta colaborativa abierta a cualquiera y que le permita registrar transacciones, de hecho, existen limitaciones en su acceso, derivadas de la necesidad de conocer las claves criptográficas y de no ser, a día de hoy, una herramienta sencilla y muy conocida. En efecto, para incorporar un nuevo bloque a la cadena es necesario conocer el *hash* del bloque anterior para incluirlo como parte del contenido que se quiere añadir. Por tanto, dejando de lado las dificultades ya mencionadas páginas atrás, cabe afirmar que las cadenas «públicas» no son tan «públicas» como inicialmente se sugiere –evidentemente, tal «sugerencia» ya no existe *ab initio* en las de carácter privado, donde el acceso es restringido pues positivamente así se busca–. Además, su carácter novedoso y las suspicacias que suscitan no ayudan a su «popularización». En tal sentido, parece que cuando se trata de activos valiosos –como, por ejemplo, podría ser la propiedad inmobiliaria– o existe el riesgo de la pérdida accidental de claves –y, con

[50] Con fundamento en el concepto de «jurisdicción distribuida», y de manera coherente con el referido carácter de las cadenas de bloques, se ha propuesto la creación de una plataforma en código abierto con un sistema para la resolución de conflictos sobre *smart contracts* y transacciones con criptomonedas que resulte descentralizado, al igual que las cadenas de bloques. Sobre esta materia, vid., por todos, KAAL y CALCATERRA, «Crypto transaction dispute resolution», *The Business Laywer*, Spring 2018.

[51] Vid. nota n.º 14.

ellas, del acceso a tales bienes– la tendencia es a confiar en «terceros de confianza» antes que en un sistema digital descentralizado[52].

En segundo lugar, las cadenas de bloques –al menos, las públicas tal y como están hoy configuradas– únicamente registran «transacciones» y no incluyen los documentos que las justifican o sirven de soporte: son cadenas de *hashes* sin que almacenen documentos[53]. Que actualmente no se incluyan de manera general no significa que no puedan hacerlo. Ahora bien, desde el punto de vista técnico, tal posibilidad traería consigo que el tamaño de los «bloques» aumentase exponencialmente, con el consiguiente incremento de costes y la mayor complejidad para el minado. Ante tal dificultad, en el *sistema Bitcoin* se ha descubierto que en cada una de las transacciones de *bitcoins* cabe almacenar además cierto número de bytes –en lo que ahora interesa, *hashes* de documentos–. A la vez, se han implementado aplicaciones externas que facilitan tal operación[54]. En Ethereum, la posibilidad de almacenar información a que aludimos ya está prevista en el propio sistema, aun cuando para el almacenaje de un documento sea necesario acudir a otras tecnologías descentralizadas[55]. De esta manera, almacenando *hashes* de documentos en las cadenas de bloques señaladas por cualquiera de las dos vías mencionadas se obtiene la ventaja de la inmutabilidad, del

[52] Cfr. NARAYANAN ET ALII, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, 2016, p. 283.

[53] En relación a lo señalado en el texto, no está demás recordar que en este trabajo usamos el término «transacción» en un sentido genérico y en él englobamos, entre otras opciones, la inclusión de un *smart contract* en la cadena de bloques, la inserción de algunas de sus variables o un pago de criptomonedas, por ejemplo. Vid., a este respecto, la nota n.º 20.

[54] La posibilidad a que aludimos en el texto fue descubierta en 2013 por ARAOZ y ORDANO, y consiste, como se dice, en crear una transacción especial en el *sistema Bitcoin* que permite almacenar el *hash* de un documento, no el documento mismo. Ahora bien, se trata de una «puerta trasera» pues el *sistema Bitcoin* está pensado para contener únicamente cuentas y transferencias de criptomonedas entre ellas. El comando que se utiliza para conseguir el efecto a que aludimos –*op return*– estaba previsto, no para almacenar *hashes* de archivos externos, sino para marcar como inválidas operaciones de gasto de *bitcoins* (cfr. TUR FAÚNDEZ, *Smart Contracts. Análisis jurídico*, Reus, Madrid, 2018, pp. 45-49). Actualmente, son varias las aplicaciones que permiten incorporar el *hash* a un bloque en *Bitcoin*. Vid., por todas, https://proofofexistence.com.

[55] Vid., por todas, las redes IPFS (https://ipfs.io) o SWARM (http://swarm-gateways.net/bzz:/theswarm.eth/), que sirven para almacenar archivos de gran tamaño y pueden constituir un complemento adecuado para las cadenas de bloques. En tales plataformas –que no usan el sistema de minado– se suben archivos y se obtiene una dirección de localización que se corresponde única y exclusivamente con el *hash* del archivo que se ha insertado en la cadena de bloques. Estas plataformas son útiles, por ejemplo, para conservar archivos asociados a «contratos inteligentes» (cfr. TUR FAÚNDEZ, *Smart Contracts. Análisis jurídico*, cit., pp. 43-45).

«sellado de tiempo» del archivo, así como del testimonio múltiple respecto de la existencia del archivo[56].

Junto con lo anterior, el almacenamiento de los documentos en la cadena de bloques –no de sus *hashes*– tiene también el inconveniente de que, al tener cada nodo una copia de todo el contenido de la cadena, se podrían estar guardando en los ordenadores de los usuarios de la red archivos ilegales –p. ej. de pornografía infantil–. Pero, dejando esta cuestión de lado, y asumiendo la posibilidad de subir archivos a una cadena de bloques, hemos de cuestionarnos por el valor y efecto que tendrían tales documentos. En este sentido, y salvo que la cadena de bloques pública dependiese de una autoridad que garantizase su contenido jurídico –lo que parece que sería una contradicción esencial con su propio concepto y finalidad–, en ningún caso podrán tener valor de escritura pública. Al no ser un funcionario público el que registra el documento, en todo caso será un documento de carácter privado y tendrá el valor propio de tal. Por lo que al Derecho español se refiere, no habría problema en su incorporación al proceso judicial pues el artículo 299 de la Ley de Enjuiciamiento Civil lo permite cuando, al señalar «*los medios de prueba de que se podrá hacer uso en juicio*», incluye los «*documentos privados*»: el documento podrá valer como medio de prueba en juicio, pero no creará un título de legitimación extrajudicial que aporte seguridad jurídica[57].

Y, en tercer lugar, no ha de olvidarse que el carácter descentralizado e inmutable de la cadena de bloques permite probar con total seguridad el momento en que una «transacción» se ha registrado; es un medio de probar que unos datos no se han modificado desde el momento específico de su incorporación a la cadena. La cadena vale, por tanto, como «sellado de tiempo», aun cuando sea un «sellado de tiempo» no cualificado –con las consecuencias jurídicas que ello tiene–, tal y como lo entiende el

[56] Cfr. TUR FAÚNDEZ, *Smart Contracts. Análisis jurídico*, cit., pp. 46-47. Como sabemos, el uso de la función *hash* a que hemos aludido servirá para comprobar si el archivo que está en el origen del *hash* incluido en la cadena de bloques ha sido alterado o no.

[57] No aporta seguridad jurídica preventiva pues, como apunta BRANCÓS, no asegura «la validez y la regularidad de las transmisiones» («El papel del notario y el *Blockchain*», *Escritura Pública*, nº 106, julio-agosto, 2017, p. 50). En este contexto, cabe mencionar que recientemente un tribunal de China (el *Internet Court* de Hangzhou) admitió como prueba en un caso de propiedad intelectual el registro de información de *blockchain* (https://bit.ly/2lMoAG6). O también la legislación, denominada *Blockchain Technology Act*, que se está tramitando en Illinois (USA) en la que se reconoce que «Section 10. (..) b) In a proceeding, evidence of a smart contract, record, or signature must not be excluded solely because a blockchain was used to create, store, or verify the smart contract, record, or signature. (c) If a law requires a record to be in writing, submission of a blockchain which electronically contains the record satisfies the law» (https://bit.ly/2Twjfpm).

Reglamento Europeo 910/2014, de 23 de julio, de Firma Electrónica (Reglamento eIDAS)[58].

En coherencia con lo anterior, cabe mencionar de nuevo el artículo 299 de la LEC, pues en su apartado tercero también alude a que «*cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias*». En lo que ahora interesa, a pesar de que el «sellado de tiempo» de la cadena de bloques no sea oficial, sí tiene valor y se puede incorporar al proceso a fin de probar la existencia de la «transacción» de que se trate. Ahora bien, ello habrá de hacerse de manera adecuada y comprensible para la otra parte y para el tribunal, para lo que –comúnmente– será necesaria la actividad pericial. En cualquier caso, como no se trata de un documento público, le resulta de aplicación el efecto que señala el artículo 1227 del Código civil: «*la fecha de un documento privado no se contará respecto de terceros sino desde el día en que hubiese sido incorporado o inscrito en un registro público, desde la muerte de cualquiera de los que lo firmaron, o desde el día en que se entregase a un funcionario público por razón de su oficio*». En definitiva, el registro en una cadena de bloques es jurídicamente un medio de prueba que, al no gozar por sí mismo de presunción de exactitud temporal e integridad del contenido –es un sellado de tiempo no cualificado-, será objeto de valoración por el juez[59].

Con todo, esta ventaja de la certeza del registro en la cadena de bloques ha de atemperarse, a nuestro juicio, por dos motivos. De una parte, por el hecho de que la incorporación de transacciones a un bloque no sigue un riguroso orden temporal; o, dicho de otra manera, no goza de ese «sellado de tiempo» de que sí goza el bloque en su incorporación a la cadena.

[58] Los sellos de tiempo no cualificados están recogidos en el artículo 41 del Reglamento Europeo de Firma Electrónica (Reglamento eIDAS) 910/2014, de 23 de julio. Son aquellos que no proceden de un prestador de servicios de confianza, que sí gozan de la presunción de exactitud de fecha y hora, así como de la integridad de los datos a que están vinculados. En consecuencia, a los documentos sellados con un sello no oficial no se le deniegan efectos jurídicos ni se excluye que sean admisibles como prueba en el proceso, pero, como a continuación se indica en el texto, serán objeto de dictamen pericial y su valor será el que aprecie el juez (en esta materia, vid. GONZÁLEZ GRANADO, «Eficacia probatoria de la *blockchain*. Criptografía y artículo 1227 del Código Civil», 25 de abril de 2016, https://bit.ly/2LQHsQ8, LLOPIS BENLLOCH, «*Blockchain* y profesión notarial», *cit.* y RAMOS MEDINA, «Propiedad intelectual, notarios y *blockchain*», 7 de diciembre de 2016, https://bit.ly/2h2GyAs).

[59] Sobre esta cuestión vid. GONZÁLEZ GRANADOS, «Eficacia probatoria de la *blockchain*. Criptografía y artículo 1227 del Código civil», *cit.*, quien específicamente se refiere en detalle al efecto del artículo 1227 CC respecto de la cadena de bloques en el ámbito contractual, de la propiedad intelectual y en el ámbito sucesorio.

De otra parte, y en otro orden de cosas, la ventaja de la función de registro ha de atemperarse también por el carácter «ciego» e inmutable de la cadena de bloques: el registro podrá probar la «transacción» registrada –su integridad y trazabilidad estarán claras–, pero nada dice del negocio que está debajo y le da sentido. En concreto, nada muestra sobre la identidad y capacidad de las partes para realizar tal negocio, de la licitud del contrato que pueda justificar tal transacción –que puede ser nulo o ilícito–, de si el consentimiento que han prestado las partes ha sido válido o en él concurrían vicios, o, en fin, de si los intervinientes tenían poder de representación suficiente y estaban legitimados para llevarla a cabo[60]. Por tanto, puede constituir un medio de prueba de la transacción registrada, pero nada aporta sobre su control jurídico o su legalidad. Entre otras cuestiones, el «sellado» lo es únicamente «de tiempo».

El razonamiento apuntado sería aplicable en caso de que en la cadena de bloques también se almacenasen documentos. Los efectivamente incluidos en ella podrían ser válidos, nulos, lícitos o ilícitos, en atención a que no existe una instancia encargada de velar por su adecuación al ordenamiento jurídico. Lo anterior salvo que hubiera una persona cualificada que tuviera tal función; pero su admisión iría en contra de la finalidad y concepto original de la cadena de bloques, que demanda la inexistencia de un órgano o intermediario que controle o supervise. Y si se pretendiese que los documentos contenidos en la cadena de bloques tuviesen validez y efectos frente a terceros, no sería prudente dejar que cualquier usuario incorporase documentos, pues es posible que su conocimiento del ordenamiento jurídico no sea completo o totalmente correcto, pudiendo generar entonces consecuencias negativas que se convertirían en «inmodificables» por la propia configuración de la cadena[61]. Inmutabilidad que ya existe actualmente aun cuando no se registren documentos: la

[60] La cadena de bloques sirve para registrar pero no aporta en la función de «control jurídico y de legalidad e información del consentimiento que aporta el notario en el documento público», motivo por el cual, «podría sustituir al registro pero no la función del notario latino-germánico» (BRANCÓS, «*Blockchain*, función notarial y registro», https://bit.ly/2TpxxUA). Por otra parte, como apunta GONZÁLEZ-MENESES (*Entender Blockchain…*, cit., p. 111) que la transferencia de valor de carácter inmutable tenga lugar por la «simple» aplicación de una clave privada a un mensaje choca «con toda una cultura jurídica (..) que, por razones tanto de respeto a la autonomía personal como de justicia material o equidad, ha venido condicionando durante siglos la validez jurídica de cualquier pretendido negocio o transacción económica a la existencia de un consentimiento real por parte del sujeto al que se imputa ese negocio, así como a la existencia de una «causa» o «consideración» legítima que justifique el desplazamiento patrimonial».

[61] Y, por los motivos apuntados en el texto, «un registro con eficacia jurídica, ya sea constitutiva o de protección al tercero, tendría poco sentido asociado al *blockchain*» al ser un sistema abierto a todos, y no todos tienen el conocimiento jurídico necesario para elaborar adecuadamente tales documentos. Y limitar quiénes podrían operar en *blockchain* constituye un contrasentido. «Un *blockchain* no abierto a todos ya no es un *blockchain*» (BRANCÓS, «*Blockchain*, función notarial y registro», *cit.*). Sobre los distintos tipos de cadenas de bloques, vid. el apartado 2 de este trabajo.

«congelación», por ejemplo, de una transacción que suponga una estafa la hace inmodificable, imposibilitando su reversión técnica *en* la cadena[62].

A modo de conclusión, cabe afirmar que actualmente la cadena de bloques no ejerce control de legalidad alguno –almacena *hashes* y no documentos– y las vías actuales para permitir que realice tal función irían en contra del sentido originario de la cadena de bloques pues el archivo de documentos con pretensión de producir determinados efectos jurídicos reclama una instancia superior controladora. En la actualidad, existen alternativas sencillas para procurar la fiabilidad y legalidad de los documentos[63]; motivo por el que no parece sencillo que, al menos en un plazo breve de tiempo, sustituyan a los Registros de derechos existentes en España[64].

[62] La transmisión no consentida de *bitcoins* podría encajarse dentro del delito de estafa del artículo 248.2.a del Código Penal: «*cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*».

[63] «Si el documento público –ya sea en relación a negocios jurídicos sobre bienes o derechos registrables, ya sea en relación a bienes y derechos no registrables– precisa de un operador específico y no está abierto a todos, resulta más simple, seguro y eficaz acudir al sistema de registro automático o semiautomático a través de la copia de la escritura pública parametrizada o al enlace de documentos notariales a través del Código Seguro de Verificación (..). Si se trata de derechos registrables, la copia parametrizada puede producir directamente la mutación registral siguiendo los principios rectores de la *direct entry* y el *registration principle*. Si se trata de derechos no registrables, el Código Seguro de Verificación permite la consulta y enlace de una escritura con su correspondiente escritura pública antecedente de la que procede el derecho» (BRANCÓS, «*Blockchain*, función notarial y registro», *cit.*).

[64] De tal opinión es ARRUÑADA, «Blockchain's Struggle to Deliver Impersonal Exchange», *cit.*, pp. 92 y ss. Lo expuesto en el texto no empece para que pudiera usarse la tecnología de la cadena de bloques como mera herramienta tecnológica que ayudase en la gestión de los Registros de derechos existentes –como cadena de bloques privada–. De todas maneras, GALLEGO FERNÁNDEZ («Cadenas de bloques y Registros de derechos», *cit.*, pp. 133 a 136) no es partidario de ello pues, según afirma, la configuración actual de los Registros y sus innovaciones tecnológicas, los hacen eficientes y operativos, gozando de uno de los más altos estándares de seguridad del mundo. Asimismo, tampoco es partidario de la incorporación de la cadena de bloques como sustitutivo del Registro –como cadena de bloques pública y autogestionada–, pues tendría más inconvenientes que ventajas. Entre otras desventajas, basta aludir ahora a que sólo garantizaría la publicidad –cuando el actual Registro además acredita el reconocimiento por el Estado de la titularidad sobre los derechos en él reflejados generando confianza a los operadores económicos–; no resolvería de manera apropiada la cuestión de la transparencia que pretende el Registro al figurar solo la «clave pública» –en el Registro actual consta la identidad real de las personas titulares de los derechos inscritos, aun cuando el acceso a los datos se restrinja a favor de quienes tengan un «*interés legítimo*» (cfr. art. 222.1 LH)–; no daría respuesta adecuada a la protección de datos, a diferencia de lo que ocurre en el Registro actual (cfr. art. 222.6 LH); el sistema de minado de bloques –aleatorio o monetario (cfr. nota n.º 24)– no respetaría el principio de prioridad, que, como es conocido, afecta al rango hipotecario aun cuando, a lo que parece, en cadenas que siguen una política FIFO –como, por ejemplo, Hyperledger fabric– se atemperaría tal inconveniente; o, finalmente y de mayor importancia, conllevaría la inexistencia de un control de legalidad y calificación, como actualmente existe en el Registro –tal problema no se resolvería tampoco con la estandarización de los contratos inscribibles pues chocaría con

### 5.4. *La identidad digital*

Ya quedó señalado que la cadena de bloques de carácter público exige por sí misma que no haya una autoridad superior que identifique a los intervinientes: es el propio sistema democratizado y consensuado el que, con su modo de operar, da garantías a los que toman parte en él. A los usuarios de las cadenas públicas –al menos, en el *sistema Bitcoin*– no les interesa primariamente que figure en la cadena quienes sean los sujetos reales específicos y particulares que intervienen en las operaciones –evidentemente, en el «mundo no virtual» sí les interesa conocer a la otra parte de la transacción–; no se exige ni interesa un registro exacto de quién está detrás de cada identificador pues lo importante es que se realicen las transacciones. Buena prueba de ello es que cualquier usuario de la cadena puede tener varios identificadores y usar uno diferente para cada transacción. Igualmente, el sellado de tiempo tampoco identifica quién sea el sujeto concreto que efectúa el registro –quién cierra el bloque– si no, en el caso que comentamos, la *dirección Bitcoin* desde la que se realiza[65].

De todas maneras, ha de tenerse presente que, a pesar de lo expuesto, por medio de mecanismos indirectos existe cierta caracterización de los números identificativos, tanto del emisor como del receptor de cualquier transacción: el seguimiento de las IP o de las cuentas, en su caso, asociadas a las operaciones –por ejemplo, un proveedor, por razones de eficiencia, mantendrá una o pocas *direcciones Bitcoin* para cobrar a sus clientes sin cambiarlas de manera habitual–, análisis de tráfico, etc.[66]. A la vista de lo

el principio de libertad de empresa (cfr. art. 38 CE) o con la libertad del juez para emitir resoluciones que tienen incidencia real en los derechos contenidos en los Registros–. Un análisis completo de cómo afecta la cadena de bloques a los Registros de derechos se contiene en GALLEGO FERNÁNDEZ, «Cadenas de bloques y Registros de derechos», *cit.*, pp. 123-136, y «Blockchains and Title Registration», *IPRA Cinder International Review*, nº 1, January-June, 2017, pp. 26-51, así como en el trabajo de ARRUÑADA, «Blockchain in Public Registries: Don't Expect Too Much», *cit.*, pp. 6-11. En definitiva, parece que la negociación de derechos reales requiere, en última instancia, de un «mínimo de ordenación pública», aun cuando ésta se limite a señalar las reglas sobre el valor de *blockchain* como evidencia judicial para la «adjudicación *in rem*» o sobre cómo resolver las divergencias entre la realidad registral y la extrarregistral (cfr. ARRUÑADA, «Limitaciones de *blockchain* en contratos y propiedad», *cit.*, pp. 2467, 2479 y 2484).

[65] Para crear una cuenta, habitualmente basta con un nombre –que puede no ser el auténtico–, un mail y una contraseña. La *dirección Bitcoin* únicamente se facilita cuando se realiza una transacción, al no existir un registro general de tales direcciones.

[66] «It may be possible to match the account number to a name using other information available online» (MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit.*; vid. Tambien TSUKERMAN, M., «The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions For The Future», 30 *Berkeley Technology Law Journal* 1127, 2015, p. 1137). Por otra parte, el anonimato derivado de que no se exija la identificación previa antes de efectuar cada operación se puede potenciar por medio del uso de sistemas que hacen la navegación en la red anónima o de mecanismos que ocultan o enmascaran las direcciones IP. Asimismo, y dando un paso más, también hay criptomonedas que ocultan la dirección de emisor y receptor y la cuantía de lo transmitido, salvo que se posea una clave de visualización; p. ej., Zcash.

anterior, cabe recordar lo que antes hemos señalado: la cadena de bloques a que aludimos no es totalmente «anónima» sino «pseudónima»[67].

Además, como en el caso que comentamos la «identidad digital» –los rasgos digitales que una persona tiene en la red, para operar en ella, y que, presuntivamente, coinciden con el sujeto, aun cuando no exista garantía de correspondencia con la identidad física– reside en las claves criptográficas explicadas, su sustracción o pérdida le imposibilitará al «verdadero titular» demostrar tal cualidad, lo que le impedirá operar con ellas en el futuro; salvo mecanismos externos a la cadena de bloques, en tales casos no será sencilla la prueba de la titularidad dentro del sistema[68]. En efecto, existe el peligro de la «pérdida de identidad digital»: al no existir una correspondencia exclusiva entre una *dirección Bitcoin* y la persona, es posible que un usuario pierda sus claves –o las olvide y no tenga copia de seguridad– o que alguien le suplante –haciéndose con sus claves de acceso al sistema; o al menos la privada, que permite el uso de la pública– y no haya modo de recuperarlas[69].

Así las cosas, y aunque la cadena de bloques permite efectuar un seguimiento riguroso de las criptomonedas envueltas en las transacciones, no ocurre lo mismo de manera absoluta respecto de quién está detrás, en este caso, de las *direcciones Bitcoin* involucradas en ellas, ni respecto de la causa de las transmisiones; lo que facilita negocios opacos o al margen de la legalidad. Con todo, según se ha dicho, al estar todas las transacciones «congeladas» cabe averiguar cierta información sobre las partes[70]. Hecho que, junto con la lógica desincentivación que genera para el uso de la cadena de bloques, no encaja adecuadamente con la normativa de protección de datos, cuando,

[67] Cfr. MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit.*

[68] Nos estamos refiriendo, según se advierte, a las cadenas de bloques públicas. Cuando se trate de una DLT privada, los elementos configuradores serán otros y no valdrá el mismo razonamiento. Por otra parte, respecto de la «identidad digital» vid., GONZÁLEZ GRANADOS, «Sólo se muere una vez: ¿Herencia digital?», 23 de diciembre de 2015, https://bit.ly/2F5elaB, quien la define como «el conjunto de rasgos digitales con el que una persona física o jurídica se muestra en la red». Y señala también que constituye un «*derecho de la personalidad* autónomo (en cuanto conceptualmente diferenciado del honor, la propia imagen, el nombre o los apellidos), y como tal, *innato, erga omnes, privado, irrenunciable y extra-patrimonial* (aún cuando en sus manifestaciones sea susceptible de valoración económica y de negocios jurídicos)». Vid. también LLOPIS BENLLOCH, «El notario ante la identidad y la capacidad digital», en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 181-189.

[69] En efecto, ni hay un registro de criptomonedas, ni hay autorizaciones de doble factor para la disposición u otros medios para evitar tal pérdida. El extravío de las claves por el usuario permite que una criptomoneda quede «perdida en el ciber espacio». Se calcula que hay más de 22 millones de euros en criptoactivos inutilizados por esta causa (cfr. ECHEBARRÍA SÁENZ, «Contratos electrónicos autoejecutables…», *cit.*, p. 87).

[70] Buena prueba de lo que se indica en el texto es que, en algunas ocasiones, se haya podido localizar a los ladrones de criptomonedas. Vid., a este respecto, STRICK, «Tracing an offshore bank and a dark web service using the blockchain — an OSINT investigation», *cit.*

como en el caso que comentamos, se trate de un sistema abierto. De tratarse de un sistema cerrado –una cadena privada–, habrá mayor opacidad, lo que garantiza la protección de datos, pero puede estimular en mayor medida acciones al margen de la legalidad. Introducir, entonces, un sistema de control en las cadenas públicas podría servir para defender la licitud de todas las transacciones y la protección de los datos incluidos en ella, pero ello iría en contra de los objetivos que se persiguen, pues, no se olvide, su uso pretende la eliminación de intermediarios innecesarios, así como de órganos supervisores.

### 5.5. *Las criptomonedas: naturaleza y función*

#### 5.5.1. Introducción

Como es conocido, *Blockchain* es la plataforma que da soporte a *bitcoin*, aun cuando lo más relevante –y que va mucho más allá de ella– es la propia metodología, concepto o herramienta de la cadena de bloques que está debajo[71]. Esta realidad no impide que haya de cuestionarse la naturaleza de las criptomonedas. En tal sentido, lo que está claro, de entrada, es que forman parte del patrimonio del que sea su titular pues se trata de un bien mueble de carácter digital susceptible de propiedad privada y de valoración económica (*arg. ex* arts. 335 y 345 CC). Su carácter patrimonial y su habilidad para el intercambio de bienes y servicios u otras operaciones, suscita el interrogante de si puede valer como medio de pago ordinario y de si es posible su transmisión *mortis causa*. Asimismo, también cabe preguntarse cómo han de hacer frente las criptomonedas al blanqueo de capitales, en atención al ya mencionado carácter «limitado» u «opaco» de las cadenas de bloques de carácter público; o, en fin, de cómo ha de afrontarse su fiscalidad[72]. Veamos cada uno de estos aspectos separadamente.

[71] En el sentido indicado en el texto se ha dicho que *bitcoin* es solamente la punta de un iceberg (cfr. FAIRFIELD, «Smart contract, bitcoin, bots and consumer protection», *cit.*, p. 38). Otras «criptomonedas» o «monedas virtuales» son Peercoin (https://peercoin.net/index.php?locale=es), Bitcoin cash (https://www.bitcoincash.org), Monero (https://getmonero.org), Dash (https://www.dash.org/es/), Litecoin (https://litecoin.org/es/) o Dogecoin (http://dogecoin.com), etc. Actualmente se estima que hay unas 1200 criptomonedas en el mundo. Una lista de las más conocidas y su capitalización se encuentra en https://coinmarketcap.com. Una comparativa de varias criptomonedas respecto de los cuatro «pasos» del pago –creación de valor, promesa de pago, realización de transacciones y almacenamiento del valor– y los actores que intervienen, se contiene en MASSACCI, NGO y WILLIAMS, «Decentralized Transaction Clearing Beyond Blockchains», (June 13, 2016), Technical report SSRN 2794913, disponible en http://dx.doi.org/10.2139/ssrn.2794913, pp. 8-16.

[72] Por otra parte, es comúnmente sabido que, además, la criptomoneda *bitcoin* se ha convertido en un instrumento de inversión especulativo con una elevada volatilidad, lo que actualmente dificulta su uso regular en los negocios.

De todas maneras, vaya por delante que, actualmente, carecemos de una normativa nacional o europea que regule de manera específica y sistemática las «monedas virtuales» –emisión, transmisión, fiscalidad, etc.–, habiendo de acudirse a legislación más general. En tal sentido, el marco normativo comunitario aplicable viene determinado, entre otras normas, por la Directiva 2009/110/CE, del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, y por la Directiva 2015/2366, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior. Y, en lo que al ámbito nacional se refiere, habremos de acudir, entre otras, a la Ley 16/2009, de 13 de noviembre, de Servicios de Pago y a la Ley de Dinero Electrónico[73].

5.5.2. ¿Son un medio de pago?

En lo que hace a la utilización de las criptomonedas como medio de pago ordinario, de entrada, ha de apuntarse que, al ser su titularidad *pseudónima* –vinculada al conocimiento de unas claves criptográficas únicas–, tiene cierta semejanza con el dinero corriente: cambia de manos y su titularidad no aparece registrada, como ocurre con algunos bienes muebles «particulares» o los inmuebles. De todas maneras, a diferencia del dinero corriente, las criptomonedas no tienen carácter fungible (*arg. ex* art. 337 CC) ni actualmente pueden ser conceptuadas como moneda de curso legal[74].

[73] A fin de no sobrecargar la redacción, incluimos aquí otra normativa aplicable, además de la que luego se mencionará en el texto. En el ámbito comunitario, el Reglamento UE 260/2012, del Parlamento Europeo y del Consejo, de 14 de marzo de 2012, por el que se establecen los requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros. Y, en el ámbito nacional, el Real Decreto 712/2010, de 28 de mayo, de régimen jurídico de los servicios de pago y de las entidades de pago, así como el Real Decreto 778/2012, de 4 de mayo, de régimen jurídico de las entidades de dinero electrónico. Por otra parte, existe un grupo de trabajo formado por la Comisión Europea y el Banco de España para el estudio de las criptomonedas y la propuesta de normativas apropiadas. Asimismo, la Agencia Estatal de Administración Tributaria ya incluía en las directrices generales de su Plan Anual de Control Tributario y Aduanero de 2018 (*BOE* nº 20, de 23 de enero de 2018) la investigación y estudio de «la incidencia fiscal de nuevas tecnologías, como *blockchain*, y, en especial, las criptomonedas», mencionando expresamente a *bitcoin* en el apartado de la prevención y represión del contrabando, narcotráfico y blanqueo de capitales. Iniciativas similares hay en otros países de la Unión.

[74] Aun cuando en el texto se señala que son infungibles por ser totalmente identificables y ser irrepetibles, cabría considerarlos como fungibles en el sentido de que en una transacción cabe reemplazar unas concretas criptomonedas por otras cualquiera sin incumplirse el requisito de identidad e integridad del pago. Tal reemplazo no supone alteración objetiva de la prestación. De esta opinión es GONZÁLEZ GRANADOS, «Retos del *BitCoin* y de la *Blockchain*», en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, p. 132.

Esto último porque no reúne los requisitos exigidos por la Ley 46/1998, de 17 de diciembre, sobre Introducción del Euro[75].

Señalado que no es una moneda oficial, tampoco puede ser reconocida como dinero electrónico pues la Ley de Dinero Electrónico especifica una serie de características en su artículo 1.2 que no son referibles a la criptomoneda. En esencia, de lo que carece es del respaldo legal del sistema financiero –no hay «*crédito contra el emisor*» (art. 1.2 LDE), pues éste, sencillamente, no existe–, y, por ello no es dinero de curso legal, ni puede serlo electrónico al no representar a ninguna divisa oficial[76].

[75] El artículo 3.1 de la Ley 46/1998, indica que «*desde el 1 de enero de 1999 inclusive, la moneda del sistema monetario nacional es el euro, tal y como esta moneda se define en el Reglamento (CE) 974/98, del Consejo de 3 de mayo*». Además de ello, hay otros dos hechos que dificultan la concepción de la criptomoneda como divisa de curso legal: su alta volatibilidad –que dificulta la función de reserva de valor propia del dinero– y que no es un «medio de cambio» ampliamente aceptado, aun cuando, cada vez, sea mayor el número de operadores que lo admite. En sentido parecido, la Dirección General de Ordenación del Juego de España –dependiente del Ministerio de Hacienda y Función Pública– señaló en la Consulta no vinculante SUG/00239, de 15 de abril de 2014, sobre apuestas con *bitcoin*, que «no puede ser considerado como una moneda de curso legal o como dinero electrónico oficial» aun cuando «es una moneda virtual convertible que puede ser intercambiada entre los usuarios» o por monedas «de curso legal o virtual». Así las cosas, en un sentido amplio –y, por lo expuesto en el texto, no técnico– cabría definir las criptomonedas como «dinero nativo digital».

[76] En concreto, el artículo 1.2 de la Ley de Dinero Electrónico dispone que es dinero electrónico «*todo valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico*». De acuerdo con el citado artículo 2.5, una operación de pago es «*una acción, iniciada por el ordenante o por el beneficiario, consistente en situar, transferir o retirar fondos, con independencia de cualesquiera obligaciones subyacentes entre ambos*». En tal sentido, ante una pregunta formulada por un Diputado de UPyD del 7 de abril de 2014, el Gobierno señaló que la criptomoneda –en tal caso, el *bitcoin*– no puede ser conceptuado como medio de pago electrónico a los efectos del artículo 34.2 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Sobre este aspecto, vid., más ampliamente, el epígrafe 5.5.4. Finalmente, vid. PACHECO JIMÉNEZ y SALES PALLARÉS, «Los medios de pago en el escenario virtual: el dinero electrónico y el *bitcoin*», en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, p. 151, donde recogen las diferencias entre las criptomonedas y el dinero electrónico; y el texto de la reciente Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, donde se señala que «las monedas virtuales no deben confundirse con el dinero electrónico, tal como se define en el artículo 2, punto 2, de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo, con el concepto más amplio de «fondos», tal como se define en el artículo 4, punto 25, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, con el valor monetario almacenado en instrumentos exentos, tal como se especifica en el artículo 3, letras k) y l), de la Directiva (UE) 2015/2366, ni con las monedas de juegos, que solo pueden utilizarse en el contexto específico de un juego. Aunque las monedas virtuales pueden utilizarse frecuentemente como medio de pago, también podrían utilizarse con otros fines y encontrar aplicaciones más amplias, tales como medios de cambio, inversión, productos de reserva de valor o uso en los casinos en línea. El objetivo de la presente Directiva es abarcar todos los posibles usos de las monedas virtuales».

A consecuencia de lo anterior, la criptomoneda puede considerarse como un bien mueble de carácter digital y divisible, irrepetible y no copiable, susceptible de ser valorado económicamente[77]. Aserto del que se derivan dos consecuencias. Primera: al ser objeto de propiedad privada, permite efectuar negocios jurídicos con ella y sobre ella. A modo de ejemplo, es posible efectuar una compraventa de criptomonedas con dinero de curso legal, o una permuta de criptomonedas por otros bienes –al no ser actualmente la criptomoneda dinero en sentido jurídico no sería una compraventa–[78]. Y segunda: al no poder ser conceptuadas las criptomonedas como monedas de curso

[77] Otras definiciones aportadas sobre *bitcoin* son: «bien patrimonial, privado, incorporal, digital, en forma de unidad de cuenta, creado mediante un sistema informático» (PABLO FERNÁNDEZ BURGUEÑO), a la que GONZÁLEZ GRANADOS añade «utilizado como medida común de valor por acuerdo de los usuarios del sistema» (cfr. GONZÁLEZ GRANADOS, «Retos del *BitCoin* y de la *Blockchain*», *cit.*, p. 132). Por otra parte, vid. el Informe sobre monedas virtuales (2016/2007(INI)) de la Comisión de Asuntos Económicos y Monetarios del Parlamento europeo (https://bit.ly/2CNzfcI) donde se indica que, aun cuando no existe una definición de aplicación universal de las criptomonedas, pueden ser consideradas –según la Autoridad Bancaria Europea (ABE)– como la «representación digital de valor no emitida por un banco central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria pero aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos». En sentido parecido, vid. FINANCIAL ACTION TASK FORCE (FATF), «Virtual currencies – key definitions and potential AML/CFT risks», June, 2014, https://bit.ly/1CXF0dj. Al constituir un bien mueble evaluable económicamente puede ser aportado para constituir una sociedad (*arg. ex* art. 58 del Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital). Vid., a modo de ejemplo, cómo fueron definidos los *bitcoins* en la primera escritura de constitución de una sociedad limitada en que se utilizaron (https://bit.ly/2To5XqH): «*Que, según dicen, un bitcóin es un bien patrimonial inmaterial «documento electrónico», objeto de derecho real, en forma de unidad de cuenta, definida mediante la tecnología informática y criptográfica denominada «Bitcoin», que permite ser utilizada como contraprestación en transacciones de todo tipo. Dichas unidades de cuenta son irrepetibles, no son susceptibles de copia y no necesitan intermediarios para su uso y disposición. Esas unidades de cuenta son de naturaleza virtual y se gestionan mediante procedimientos informáticos y a través de ciertas claves públicas y privadas, que permiten la transmisión de dichos bitcóins entre cuentas abiertas*».

[78] A nuestro juicio, cabe derecho de propiedad sobre una criptomoneda, pues su titular tiene un poder directo e inmediato sobre el bien –en este caso, digital– frente a terceros. Y, al existir dicha titularidad, resultan embargables. Ahora bien, en relación con la embargabilidad surge un problema práctico que consiste en cómo obtener las claves para proceder al embargo, pues, a tal fin, no cabe forzar la voluntad del titular, y, en el caso del *sistema Bitcoin*, no existe un registro general de los *bitcoins* con sus titulares correspondientes (negando, únicamente en la dimensión práctica, la incoercibilidad y la embargabilidad, vid., GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., p. 72; por otra parte, vid. el Auto de 23 de julio de 2018 de la Audiencia Provincial de Pontevedra (JUR 2018, 295137) respecto de una venta de *bitcoins* «autorizada» por el juzgado y su posterior embargo). En este sentido, como se ha dicho, el *bitcoin* recuerda al dinero efectivo, siendo la posesión la que determina la titularidad. Y, al igual que el dinero efectivo, puede ser considerado como dinero fiduciario (respecto de la asimilación de la criptomoneda al dinero efectivo por razón de su irreivindicabilidad vid. GONZÁLEZ-MENESES, *Entender Blockchain…*, cit., pp. 109-110). Por otra parte, acudiendo a la teoría del título y el modo para explicar cómo opera la transmisión de la propiedad de un *bitcoin* aun cuando no haya desplazamiento físico del bien, vid. GOMÁ GARCÉS, «La transmisión de la propiedad de *Bitcoin*», 28 de junio de 2015, https://bit.ly/2F6vmkU. A su juicio, el *título* sería la exhibición de la clave pública, y el *modo* el registro en la cadena de bloques que funcionaría a modo de *traditio simbólica*.

legal –y, por tanto, no formar parte del sistema monetario–, no constituyen una deuda de dinero ni han de ser aceptadas como medio de pago de las deudas de tal clase (arg. *ex art.* 1170 CC)[79]. Lo cual no impide que, en virtud de la libertad de las partes, puedan ser aceptadas como medio de pago de la obligación de que se trate a modo de dación en pago (*arg. ex* art. 1166 CC)[80].

5.5.3. La transmisión *mortis causa* de las criptomonedas

Admitida la transmisión *inter vivos* de las criptomonedas, ¿qué sucede con la que se efectúa *mortis causa*? De entrada, nada parece impedirla, y al ser un bien que forma parte del patrimonio del causante habrá de seguir las reglas generales. Ahora bien, aun cuando sea posible, se trata de un bien peculiar, y, por ello, la especialidad que en este ámbito caracteriza a las criptomonedas y que consiste en el conocimiento de las claves de acceso al monedero virtual o *wallet* que habilita para disponer de ellas debe acomodarse a la normativa. Ordinariamente, el único que conoce tales claves y puede

[79] La obligación de pago de criptomonedas habría de considerarse no una obligación genérica como las dinerarias –no es reconocido como dinero legal; todo lo más como «dinero privado» (cfr. TUR FAÚNDEZ, *Smart Contracts. Análisis jurídico*, cit., p. 132)– sino de género limitado, aplicándosele el régimen correspondiente: restricción del brocardo *genus numquam perit*, juega el caso fortuito o la fuerza mayor en el supuesto de imposibilidad sobrevenida del cumplimiento, etc. Asimismo, tampoco podría acudirse a un procedimiento monitorio, al exigir el artículo 812 LEC que se trate del «*pago de deuda dineraria de cualquier importe, líquida, determinada, vencida y exigible*». Por otra parte, no parece que la criptomoneda pueda ser considerada como título-valor al carecer de reconocimiento legal y al carecer también de emisor –no hay deudor ni derecho ejercitable frente al «emisor»–. En otro orden de cosas, LLOPIS BENLLOCH, («*Bitcoin* como medio de pago en la compra de bienes», 19 de diciembre de 2017, https://bit.ly/2Jv0YmL), analizando el uso de *bitcoins* en la compraventa de inmuebles, admite que «no hay una única posición positiva acerca de su configuración legal y jurídica», existiendo, en cambio una «posición común negativa» que consiste en no reconocerlos como moneda de curso legal ni dinero electrónico. Tras ello, se pregunta si pueden ser «*signo que represente*» al dinero *ex artículo* 1445 CC. En tal sentido, concluye que no es posible de acuerdo con el concepto estricto de dinero, pero sí podría serlo en atención a su reconocimiento como medio de pago y las consecuencias tributarias que genera. Además, señala que en atención a que, generalmente, las criptomonedas se utilizan para adquirir bienes o derechos o contratar servicios, parece que «desde este punto de vista no sería tan descabellado pensar que las criptomonedas, con sus peculiaridades, pudieran ser directamente consideradas como signo que, de manera mediata, representa dinero, sobre todo si se llega a asimilar legalmente en España o Europa al pago mediante efectivo metálico, aunque no se le atribuya por ello la condición de dinero». Ahora bien, la consideración como pago en metálico, haría aplicable al «pago con criptomonedas» la Ley 7/2012, de 29 de octubre, de modificación de la normativa tributaria y presupuestaria y de adecuación de la normativa financiera para la intensificación de las actuaciones en la prevención y lucha contra el fraude y la conocida limitación de los 2.500 euros para pagos de tal clase; lo que, evidentemente, le restaría aplicación práctica, impidiendo su popularización.

[80] El Código civil reconoce al pago el efecto liberatorio de una obligación (cfr. art. 1156 CC) y deja libertad a las partes para establecer de común acuerdo su objeto, señalar el instrumento por medio del que se efectuará –p. ej. dinero electrónico, cheque, pagaré, etc.–, o, en fin, acordar una alteración sobre él. De otra parte, negando que los «mineros» puedan ser considerados como entidades de pago a efectos de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, vid. ECHEBARRÍA SÁENZ, «Contratos electrónicos autoejecutables…», *cit.*, pp. 91-92.

acceder a la moneda virtual es su titular. Así, la inclusión de las claves en un testamento supondrá hacerlas públicas, permitiendo el acceso y la «apropiación» de las criptomonedas a todos los que puedan acceder al testamento original o puedan obtener una copia de dicho instrumento, sean o no las personas a quienes se les hubiese querido dejar tales bienes. En efecto, tratándose de un testamento abierto notarial –el mayoritario en España–, de acuerdo con el artículo 226 del Reglamento Notarial, «*fallecido el testador, tendrán derecho a copia: a) Los herederos instituidos, los legatarios, albaceas, contadores partidores, administradores y demás personas a quienes en el testamento se reconozca algún derecho o facultad; b) Las personas que, de no existir el testamento o ser nulo, serían llamados en todo o en parte en la herencia del causante (..), c) Los legitimarios*».

El problema apuntado –que no resulta totalmente novedoso pues algo similar ocurre con claves de cajas fuertes u otros elementos digitales como, por ejemplo, perfiles en redes sociales– podría solventarse por medio de la elaboración de una segunda escritura donde figuren las claves criptográficas cuyo acceso esté reservado únicamente, por expresa disposición del testador, al heredero o legatario a quien se le haya querido beneficiar con las criptomonedas –no solucionaría el problema señalado la mera existencia de una segunda escritura si no consta la restricción de acceso mencionada–. Esta segunda escritura podría ser, por ejemplo, otro testamento –aclaratorio o complementario, y, por tanto, sin efecto revocatorio del anterior–, un acta notarial de manifestaciones, o un acta de protocolización o incluso de depósito notarial. Resuelto, por tanto, el problema apuntado, surgirá otro nuevo consistente en el interés de los demás partícipes en la herencia en conocer el número y el valor de las criptomonedas, a fin de cuantificar el patrimonio del causante, y, entre otras cosas, determinar las legítimas –si existen– o pagar a los eventuales acreedores[81]. A nuestro juicio, la resolución de este segundo problema pasa por el desempeño de las funciones propias por parte del albacea y, en su defecto, del heredero.

Cuando no haya mención a las criptomonedas en el testamento o se abra la sucesión intestada, será el albacea o el heredero el que deberá indagar por los elementos que conforman el patrimonio del causante. En tal sentido, las criptomonedas actuarían como los demás bienes: de no probarse su existencia –en este caso, de no conocerse su existencia o las claves que permiten disponer de ellas– no se incluirá en el inventario de la herencia, a efectos de su posterior reparto y entrega.

[81] Sobre esta cuestión, vid. LLOPIS BENLLOCH, «Herencias con *bitcoin*, un caso de futuro», 31 de julio de 2014, https://bit.ly/2K78EI4, quien también menciona que la limitación del acceso a la copia no puede afectar al heredero, y, a la vez, alude al problema de valoración de la criptomoneda.

### 5.5.4. Las criptomonedas y el blanqueo de capitales

En lo que se refiere a la prevención del blanqueo de capitales, existen tres hechos que pueden facilitar que las operaciones con monedas virtuales se utilicen para tal actividad ilícita: el carácter pseudónimo de la cadena de bloques que le dota de cierta opacidad a efectos de evitar el blanqueo[82]; que las criptomonedas no sean consideradas divisas, lo que, de entrada, las excluye de la normativa de prevención de blanqueo; y que hasta hace poco tiempo no existiese ninguna mención expresa a las criptomonedas –ni, en concreto, al *bitcoin*– en la normativa. En efecto, hasta la actual Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, no se aludía positivamente a las criptomonedas, aunque sí hubiese recomendaciones a las autoridades de los países miembros para que utilizasen la normativa nacional sobre blanqueo de capitales –y se adaptase, de ser el caso– para su aplicación a las operaciones con monedas virtuales[83]. Así las cosas, la nueva Directiva sobre blanqueo de capitales exige que los «*exchangers*» y los proveedores de *wallets* introduzcan procedimientos de verificación de identidad –*know your costumer*, KYC– haciendo uso, si es posible, de los mecanismos previstos en el Reglamento eIDAS (art. 2.1.3 g y h de la Directiva), así como que soliciten el registro para poder seguir proveyendo tales servicios (art. 47.1 de la Directiva)[84].

En lo atinente a España, hasta la implementación de la Directiva aprobada ha de utilizarse la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, que no contiene ninguna referencia expresa a las

[82] Aun cuando la opacidad de la cadena de bloques pueda facilitar el blanqueo, centrarse únicamente en uno de los riesgos de dicha «tecnología», resulta, cuando menos, un análisis parcial de la realidad. Y ello aun a pesar de que pueda existir una sensación –más o menos generalizada– de que *bitcoin* está vinculado ordinariamente a negocios fraudulentos o ilegales, quizá por casos pasados como Silk Road –mercado en el que se realizaba negocios ilegales cerrado el 2 de octubre de 2013 por el FBI– o MtGox, el mayor *exchanger* de *bitcoins* que finalmente quebró. En este ámbito, existen variados estudios que señalan que la actividad con *bitcoins* no se sustenta mayoritariamente en actividades ilegales, y otros que inciden en lo contrario.

[83] Cfr. Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. La nueva Directiva modifica la anterior siguiendo lo señalado por el Plan de acción del Parlamento Europeo y del Consejo para fortalecer la lucha contra la financiación del terrorismo (*Action Plan for strengthening the fight against terrorist financing*, Strasbourg, 2.2.2016 COM(2016) 50 final, p. 5) que sugiere lo siguiente: «as a first step the Commission will propose to bring anonymous currency exchanges under the control of competent authorities by extending the scope of the AMLD (Anti-Money Laundering Directive) to include virtual currency exchange platforms and have them supervised under Anti-Money Laundering / countering terrorist financing legislation at national level».

[84] Asimismo, incluye una definición de «monedas virtuales» y de «proveedor de servicios de custodia de monederos electrónicos» en el artículo 3 de la Directiva, números 18 y 19.

monedas virtuales[85]. De todos modos, creemos que la ausencia de mención específica no impide que las criptomonedas puedan entenderse incluidas dentro del artículo 16 de dicha ley, si se las considera como mercancía[86]. Igualmente, también quedaría al amparo de dicha normativa la actividad comercial desarrollada «*profesionalmente con bienes en los términos establecidos en el artículo 38*» (cfr. art. 2.1.w Ley 10/2010), que alude a las transacciones que usen «medios de pago» reconocidos por el artículo 34.2 de la misma ley por importe superior a 15.000 euros –ya sea en una única operación o en varias, si hay vinculación entre ellas–[87]. Por tanto, si como hemos hecho, se reconocen las criptomonedas como medios de pago, aun a pesar de que no exista referencia expresa a ellas en la Ley 10/2010, sí le resultaría de aplicación dicha normativa[88].

Siendo ello así, ya existe algún pronunciamiento de los tribunales españoles que aplica a las criptomonedas la referida Ley de prevención del blanqueo de capitales. En

[85] El reglamento de la ley señalada en el texto fue aprobado por medio de Real Decreto 304/2014, de 5 de mayo.

[86] En concreto, el artículo 16 de la Ley 10/2010, dispone que «*los sujetos obligados prestarán especial atención a todo riesgo de blanqueo de capitales o de financiación del terrorismo que pueda derivarse de productos u operaciones propicias al anonimato, o de nuevos desarrollos tecnológicos, y tomarán medidas adecuadas a fin de impedir su uso para fines de blanqueo de capitales o de financiación del terrorismo. En tales casos, los sujetos obligados efectuarán un análisis específico de los posibles riesgos en relación con el blanqueo de capitales o la financiación del terrorismo, que deberá documentarse y estar a disposición de las autoridades competentes*».

[87] El artículo 34.2 de la Ley 10/2010, considera que «*a los efectos de esta Ley se entenderá por medios de pago: (..) c) Cualquier otro medio físico, incluidos los electrónicos, concebido para ser utilizado como medio de pago al portador*». Por su parte, LLOPIS BENLLOCH («*Bitcoin* como medio de pago en la compra de bienes», *cit.*) tras considerar las criptomonedas como medios de pago –y, por tanto, sujetos a la Ley a que ahora aludimos– menciona que, a efectos notariales, el artículo 177 del Reglamento Notarial ya obligaba a detallar en la escritura los medios de pago utilizados a fin de prevenir el fraude fiscal, aun antes de las disposiciones establecidas por la Ley de Blanqueo de Capitales de 2010. En concreto, el precepto señalado dispone que «*en las escrituras públicas relativas a actos o contratos por los que se declaren, constituyan, transmitan, graven, modifiquen o extingan a título oneroso el dominio y los demás derechos reales sobre bienes inmuebles, se identificarán, cuando la contraprestación consistiera, en todo o en parte, en dinero o signo que lo represente, los medios de pago empleados por las partes, en los términos previstos en el artículo 24 de la Ley del Notariado, de acuerdo con las siguientes reglas*». Por su parte, GONZÁLEZ GRANADOS («Retos del *BitCoin* y de la *Blockchain*», *cit.*, p. 135), entiende que las empresas de *bitcoin* estarían incluidas en la Ley 10/2010, de Blanqueo de capitales, pues pueden ser conceptuadas como «*personas que ejerzan profesionalmente actividades de cambio de moneda*» (cfr. art. 2.1.i).

[88] Vid., en este sentido, las Resoluciones vinculantes V1028-15 y V1029-15 de la Dirección General de Tributos de 30 de marzo de 2015, a las que luego nos referiremos. Lo expuesto en el texto tiene como consecuencia que, al menos a ciertos efectos fiscales, el intercambio de bienes por *bitcoins* no será una permuta sino una compraventa. Tal aserto ha sido reconocido por la DGT únicamente en relación al IVA. Respecto del resto de impuestos, a día de hoy, no hay pronunciamiento expreso, aunque todo apunta a que, de efectuarse las oportunas consultas, la DGT señalará también que se tratará de una compraventa y no de una permuta, cambiando así la interpretación inicial transmitida a los inspectores de dicho ámbito.

concreto, se trata de la sentencia de la Audiencia Provincial de Asturias de 6 de febrero de 2015 (JUR 2015, 66556), que admitió la resolución de un contrato por parte de una entidad bancaria. En el supuesto planteado, se había firmado un contrato de afiliación a los sistemas de tarjetas Visa y MasterCard, que incluía la instalación de un terminal de punto de venta (TPV) para la adquisición de *bitcoins* por medio de tarjetas de crédito. El apoyo normativo en que la sentencia basa la resolución del contrato existente es el artículo 7.3 de la Ley 10/2010, ante la imposibilidad de la entidad bancaria de garantizar las medidas de diligencia impuestas por la referida norma[89]. Como es conocido, estas medidas son especialmente reforzadas cuando se trata de productos u operaciones propicias al anonimato y nuevos desarrollos tecnológicos –p. ej., por la imposibilidad de verificar la legitimidad y el origen de los fondos– (cfr. arts. 6, 12 y 16 Ley 10/2010). La consecuencia que cabe extraer de la sentencia reseñada es que las entidades que se dediquen a compraventa e intercambio de criptomonedas –en el caso mencionado, *bitcoin*– habrán de cumplir lo establecido por la Ley 10/2010, de prevención del blanqueo de capitales, para continuar con tales operaciones[90].

5.5.5. La fiscalidad de las criptomonedas

Una última cuestión relativa a las criptomonedas es la que atañe a su fiscalidad. De entrada, se ha de apuntar que no parece fácilmente conciliable el uso de las criptomonedas en una cadena de bloques «pseudónima» y transnacional con el mecanismo general de liquidación y recaudación de impuestos, que se caracteriza por la identificación de cada persona singular, por su ámbito nacional y por un notable control estatal de los movimientos de capitales y la actividad económica[91]. Expuesto lo

[89] En concreto, el artículo 7.3 de la Ley 10/2010 dispone que «*los sujetos obligados no establecerán relaciones de negocio ni ejecutarán operaciones cuando no puedan aplicar las medidas de diligencia debida previstas en esta Ley. Cuando se aprecie la imposibilidad en el curso de la relación de negocios, los sujetos obligados pondrán fin a la misma, procediendo a realizar el examen especial a que se refiere el artículo 17. La negativa a establecer relaciones de negocio o a ejecutar operaciones o la terminación de la relación de negocios por imposibilidad de aplicar las medidas de diligencia debida previstas en esta Ley no conllevará, salvo que medie enriquecimiento injusto, ningún tipo de responsabilidad para los sujetos obligados*».

[90] En materia de prevención de blanqueo de capitales, algunas recomendaciones sobre políticas a implementar, así como sobre el establecimiento de los controles tecnológicos necesarios para un buen funcionamiento con *bitcoin*, se contienen en RAMOS SUÁREZ, «La prevención del blanqueo de capitales y el *Bitcoin*», 18 de septiembre de 2015, https://bit.ly/2C0oS3w.

[91] Quizá, al no ser posible localizar la cadena de bloques en una jurisdicción –es una red de nodos descentralizada por todo el globo–, sí resulte más sencillo con los *bitcoins*. En tal sentido, cabría localizarlos donde resida su titular. Si son varios y de diversos países, quizá donde resida el que tenga el control sobre las claves del monedero –p. ej. si es una empresa–. Ahora bien, esto no resolvería el problema si se trata de claves multifirma –al modo de las cuentas bancarias mancomunadas–. A lo que parece, es necesaria una regulación que resuelva, entre otros, el problema mencionado. De todas maneras, como se indica en el texto, no parece fácilmente conciliable el actual sistema tributario con una

anterior, a continuación, aludiremos a dos operaciones –el minado y la compraventa de criptomonedas– pues su sujeción impositiva ha sido resuelta en varias Consultas vinculantes de la Dirección General de Tributos, dependiente del Ministerio de Hacienda y Función Pública. Tras ello, efectuaremos un repaso de cómo tributan las criptomonedas respecto de los impuestos más frecuentes.

Como se ha apuntado, la labor de minado tiene la finalidad de cerrar y añadir bloques a la cadena. Como «recompensa», el que la realiza recibe cierta cantidad de *bitcoins* creados por el propio sistema. Así las cosas, en la Consulta vinculante V3625-16, de 31 de agosto de 2016, la Dirección General de Tributos acude al artículo 4.1 de la Ley 37/1992, de 28 de diciembre, del IVA, para determinar si dicha labor está sujeta o no al impuesto. En concreto, el citado precepto dispone que «*estarán sujetas al impuesto las entregas de bienes y prestaciones de servicios realizadas en el ámbito espacial del impuesto por empresarios o profesionales a título oneroso, con carácter habitual u ocasional, en el desarrollo de su actividad empresarial o profesional…*». Dejando de lado la consideración de qué sea empresario, y aceptado que la actividad se realiza dentro del ámbito espacial de aplicación el impuesto, la Dirección General centra su atención para resolver la cuestión planteada en el carácter oneroso o no de la actividad[92]. Y, tomando apoyo en los Asuntos C-154/1980 y C-16/1993 del Tribunal de Justicia de la Unión Europea, concluye que en la actividad de minado no existe una relación entre el proveedor del servicio –el minero– y el destinatario de dicho servicio, ni tampoco que la retribución que recibe aquél sea el «contravalor» por el servicio prestado. Lo anterior, porque en la actividad realizada por los mineros no cabe identificar un destinatario o cliente efectivo, al ser las criptomonedas con que se les recompensa generadas por el mismo sistema[93]. La consecuencia que deduce la Dirección General es que la actividad de minado no está sujeta al IVA.

---

economía basada en *blockchain*, donde el aparato estatal tiene menos control sobre los movimientos y operaciones económicas. Apuntando la necesidad de un cambio radical de enfoque en relación a los impuestos, vid. CARRASCOSA COBOS, «Cryptocurrencies may finish with tax systems as we know them», 4 de febrero de 2018, https://bit.ly/2CiZQOd.

[92] El artículo 4.3 de la misma Ley indica que la sujeción al IVA se produce con independencia de los fines o resultados perseguidos en la actividad empresarial o profesional o en cada operación en particular. Asimismo, el artículo 5.1 y 5.2 de la Ley del IVA, definen el concepto de empresario y las actividades empresariales o profesionales a los efectos del impuesto.

[93] De acuerdo con la sentencia del TJUE, de 5 de febrero de 1981 –Asunto C-154/1980 de *Coöperatieve Aardappelenbewaarplaats*–, para considerar que una prestación de servicios se realiza a título oneroso –y, por tanto, esté sujeta al IVA *ex artículo* 4.1 Ley 37/1992– «debe existir una relación directa entre el servicio prestado y la contraprestación recibida». Asimismo, el 3 de marzo de 1994, en la sentencia R. J. Tolsma, Asunto C-16/1993, el TJUE precisa que la prestación de servicios se efectúa a título oneroso –y, por tanto, es imponible– si entre quien realiza la prestación y el destinatario existe «una relación jurídica en cuyo marco se intercambian prestaciones recíprocas y la retribución percibida por quien efectúa la

La sujeción de la transmisión de criptomonedas al IVA también ha sido resuelta en varias Consultas vinculantes de la Dirección General de Tributos (V1028-15, V1029-15, V2846-15, de 30 de marzo y de 1 de octubre de 2015). En las citadas Consultas se concluye que la actividad de compraventa de criptomonedas –en el caso planteado, *bitcoin*– a través de cajeros o máquinas de *vending*, sí está sujeta al IVA. Ello por cuanto reúne los requisitos señalados por el artículo 4.1 de la Ley del IVA, anteriormente transcrito: es una entrega de bienes en el ámbito espacial del impuesto efectuada por un empresario o profesional a título oneroso en el desarrollo de su actividad. Señalado lo anterior, la Dirección General apunta que, a pesar de estar sujeto a IVA, su transmisión está exenta pues el artículo 20.1.18 h) e i) de la citada ley exime las operaciones «*relativas a transferencias, giros, cheques, libranzas, pagarés, letras de cambio, tarjetas de pago o de crédito y otras órdenes de pago*»[94]. Y por «*otras órdenes de pago*» –u «*otros efectos comerciales*» según el texto de la Directiva origen de la Ley– ha de entenderse, de acuerdo con la sentencia C-461/12, *Granton Advertising* del Tribunal de Justicia de la Unión Europea, aquellos derechos que, sin ser un crédito o un cheque, confieran un derecho a una determinada cantidad de dinero; esto es, instrumentos de pago que permiten la transferencia de dinero. Concepto dentro del que cabe incluir a *bitcoin*, pues, según la Dirección General, a efectos fiscales actúa como medio de pago y, por sus propias características, deben entenderse incluidos

prestación constituye el contravalor efectivo del servicio prestado al destinatario». Aspectos que, como se apunta en el texto, no concurren en la actividad de minado.

[94] Se traspone así el artículo 135.1.d de la Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del IVA que eximía las operaciones «*incluida la negociación, relativas a depósitos de fondos, cuentas corrientes, pagos, giros, créditos, cheques y otros efectos comerciales, con excepción del cobro de créditos*». De todos modos, parece más correcto, de acuerdo con la Sentencia del Tribunal de Justicia de la Unión Europea (Sala Quinta), de 22 de octubre de 2015 –Asunto C-264/14, caso *Skatteverket* contra *David Hedqvist*– eximir las criptomonedas por la vía del artículo 135.1.e de la Directiva cuando se refiere a divisas y medios de pago. Y es que según el Abogado General «el objetivo del artículo 135, apartado 1, letra e, de la Directiva del IVA es permitir que todas las divisas se puedan convertir con el menor coste posible, en aras de una fluida circulación de pagos». A este respecto, la última sentencia citada señala que «pues bien, las operaciones relativas a divisas no tradicionales (…) constituyen operaciones financieras siempre que tales divisas hayan sido aceptadas por las partes de una transacción como medio de pago alternativo a los medios legales de pago y no tengan ninguna finalidad distinta de la de ser un medio de pago. (...) Así pues, del contexto y de la finalidad de dicho artículo 135, apartado 1, letra e, se deduce que interpretar esta disposición en el sentido de que se refiere únicamente a las operaciones relativas a las divisas tradicionales equivaldría a privarla de una parte de sus efectos. En el litigio principal consta que la divisa virtual «bitcoin» no tiene ninguna finalidad distinta de la de ser un medio de pago y que ciertos operadores la aceptan como tal. En consecuencia, procede concluir que el artículo 135, apartado 1, letra e, de la Directiva del IVA se refiere igualmente a unas prestaciones de servicios como las controvertidas en el litigio principal, consistentes en un intercambio de divisas tradicionales por unidades de la divisa virtual «bitcoin», y viceversa, y realizadas a cambio del pago de un importe equivalente al margen constituido por la diferencia entre, por una parte, el precio al que el operador de que se trate compre las divisas y, por otra, el precio al que las venda a sus clientes». Según se advierte, se exime del IVA a las criptomonedas en virtud de un artículo diverso del que lo hace la Dirección General de Tributos.

dentro del concepto de «*otros efectos comerciales*». Por lo tanto, la transmisión está sujeta a IVA, pero exenta. Asimismo, cuando el empresario únicamente realice operaciones sujetas a IVA, pero exentas –incluidas en los artículos 20 y 26 de la Ley 37/1992–, no está obligado a presentar las declaraciones-liquidaciones que exige el Reglamento del IVA (art. 71 RD 1624/1992, de 30 de diciembre)[95].

En ninguno de los casos señalados –actividad de minado y compraventa de criptomonedas– se genera el derecho a deducir las cuotas del IVA soportadas, pues, se trata, según se ha dicho, de operaciones no sujetas al impuesto –el minado– o sujetas pero exentas –la transmisión de *bitcoins*– (cfr. art. 94. Uno de la Ley 37/1992)[96].

Asimismo, la Dirección General concluye también que en los dos casos mencionados es preciso darse de alta en el Impuesto sobre Actividades Económicas. Ello por cuanto, el «*mero ejercicio, en territorio nacional, de actividades empresariales*» –sea o no habitual, exista o no lucro, se realice o no en un local determinado, se halle o no especificada en las tarifas del impuesto– constituye el hecho imponible del dicho Impuesto (cfr. art. 78.1 RD Legislativo 2/2004, de 5 de marzo, que aprueba el TR de la Ley Reguladora de las Haciendas Locales)[97]. Expuesto lo anterior, veamos de manera sucinta qué sucede con el resto de impuestos.

En lo que hace al Impuesto sobre la Renta de las Personas Físicas, y siempre que no se consigan en el desarrollo de una actividad económica, las rentas que se obtengan de la transmisión de criptomonedas se conceptúan como ganancias patrimoniales[98].

[95] La obligación de presentar tales declaraciones-liquidaciones está contenida en el artículo 164.6 de la Ley 37/1992.

[96] Aun cuando lo expuesto en el texto pueda parecer beneficioso, no ha de olvidarse que el «minero» no puede deducir el IVA soportado en la inversión que realiza: materiales, equipos informáticos, electricidad, etc. Por otro lado, como a continuación se señala en el texto, los mineros han de darse de alta como autónomos en el Impuesto de Actividades Económicas y en la Seguridad social. Los ingresos o rentas que perciban por el desarrollo de tal actividad estarán sujetos al IRPF o al Impuesto de Sociedades, según los casos.

[97] Ninguna de las actividades mencionadas en el texto está especificada en las tarifas del impuesto, con lo que se clasificarán, provisionalmente, en el grupo o epígrafe correspondiente a la actividad a la que por su naturaleza más se asemejen, y tributarán por la cuota asignada a ésta. En lo que hace a la actividad de minado, se clasifica en el epígrafe 831.9 de la Sección Primera –«*otros servicios financieros n.c.o.p*»–. Y, respecto de la compraventa de *bitcoins*, en el epígrafe 969.7 de la Sección Primera –«*otras máquinas automáticas*»–.

[98] La Consulta vinculante de la Dirección General de Tributos 0999-18, de 18 de abril de 2018, señala que las permutas entre criptomonedas también están sujetas a tributación a efectos del IRPF: «el intercambio entre monedas virtuales diferentes realizado por el contribuyente al margen de una actividad económica da lugar a la obtención de renta que se califica como ganancia o pérdida patrimonial conforme al citado artículo 33.1». Vid. también la consulta vinculante de la Dirección General de Tributos 1149-18, de 8 de mayo de 2018, donde señala que no se aplica a las monedas virtuales el régimen de

Cuestión distinta será si forman parte de la Renta de Ahorro o la General, según se consideren las criptomonedas como «*elementos patrimoniales*» (art. 46 de la Ley 35/2006, de 28 de noviembre, del IRPF) o como medios de pago[99].

Respecto del Impuesto de Sociedades, tributarán conforme a él tanto las ganancias que provengan de la transmisión de criptomonedas como los ingresos derivados de las actividades profesionales vinculadas a tales operaciones. Y es que la Consulta V2228-13, de 8 de julio de 2013, señaló que «formarán parte de la base imponible del impuesto sobre sociedades, los ingresos devengados en cada período impositivo derivados de los servicios prestados por la consultante –un *exchanger*– en concepto de comisión, tanto en las operaciones de compraventa de moneda virtual como en las operaciones de recarga de tarjetas de crédito virtuales».

Por lo que atañe al Impuesto de Patrimonio, la consideración de las criptomonedas como bienes de carácter patrimonial susceptibles de valoración económica conlleva que deban ser incluidas en la base imponible del impuesto, con la valoración de mercado que tengan a fecha de 31 de diciembre de cada período impositivo (cfr. arts. 1 y 29 de la Ley 19/1991, de 6 de junio, del Impuesto sobre el Patrimonio)[100].

---

ganancias patrimoniales del artículo 95 bis.1 de la LIRPF cuando exista cambio de residencia al no tener aquéllas la consideración de «*acciones o participaciones de cualquier tipo de entidad*».

[99] La no entrega en el plazo acordado de los *bitcoins* debidos –sea cual fuere la causa: quiebra del *exchanger*, estafa, etc.– únicamente computará como pérdida patrimonial a efectos del IRPF cuando se cumpla alguno de los requisitos señalados por el artículo 14.2.k de la Ley del IRPF. Si posteriormente se entregan computarán como ganancial patrimonial. En este sentido, la Consulta de la Dirección General de Tributos V2466-08, de 22 de diciembre de 2008, señaló que se considera como ganancia patrimonial la obtenida en la diferencia de cambio. Cuando se refieren a divisas, el momento de tributación se sitúa en el cambio efectivo a euros (cfr. art. 14.1.c y 14.2.e de la Ley del IRPF). Ahora bien, según señala LLOPIS BENLLOCH («*Bitcoin* como medio de pago en la compra de bienes», *cit.*), trasladar el momento de tributación de la ganancia patrimonial derivada de la criptomoneda a su conversión en dinero podría generar situaciones injustas: es posible que quien haya generado y disfrutado del aumento de valor sea el transmitente que paga un servicio utilizando la criptomoneda, y sea el adquirente el que la convierta en dinero. Por tal motivo, recomienda dividir en dos el tramo gravable del aumento de valor. En este contexto, la Consulta Vinculante de la Dirección General de Tributos 0808-18, de 22 de marzo, indica que «la alteración patrimonial habrá de entenderse producida en el momento en que se proceda a la entrega de las monedas virtuales por el contribuyente en virtud del contrato de compraventa, con independencia del momento en que se perciba el precio de la venta, debiendo, por tanto, imputarse las ganancia o pérdida patrimonial producida al período impositivo en que se haya realizado dicha entrega». Según se advierte, toma como momento relevante el que se refiere a la orden de vender y no tanto el en que se recibe el dinero. En cualquier caso, sea cual fuere el modo de tributación, lo que parece claro es que al usuario medio no le resultará sencillo obtener la información y documentación necesaria para acreditar las pérdidas y ganancias.

[100] Vid., sobre esta cuestión, la Consulta vinculante de la Dirección General de Tributos V0250-18, de 1 de febrero de 2018, donde se señala que «el hecho imponible del impuesto está constituido para el sujeto pasivo y en el momento del devengo, de la titularidad del conjunto de bienes y derechos de contenido económico que le sean atribuibles, con deducción de cargas y gravámenes que disminuyan su valor y de

Finalmente, respecto del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados que grava la compraventa de bienes y derechos entre particulares, teniendo en cuenta que aún no existen consultas vinculantes no resulta sencillo determinar si la adquisición de criptomonedas está exenta o no. De todos modos, parece que la adquisición de *bitcoins* ha de considerarse, mientras la Dirección General de Tributos no señale lo contrario, una operación sujeta y no exenta al ITP. Respecto de las compraventas realizadas utilizando criptomonedas, si se considera que se trata de «*entregas de dinero que constituyan el precio de bienes o se verifiquen en pago de servicios profesionales*», tales operaciones estarían exentas en la modalidad de transmisiones patrimoniales onerosas (cfr. art. 45. I.B.4º del RD Legislativo 1/1993, de 24 de septiembre, por el que se aprueba el TR de la Ley del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados). Si, en cambio, tal operación se califica como permuta, deberá tributar. A día de hoy no existe aún una Consulta vinculante de la DGT que resuelva tal cuestión, aunque todo apunta a que cuando lo haga, no lo hará en el segundo sentido[101].

---

la deudas y obligaciones personales de las que deba responder». En consecuencia, las criptomonedas «deberán declararse en el impuesto sobre el Patrimonio por su precio de mercado determinado a fecha de devengo (31 de diciembre de cada año) de acuerdo, respectivamente, con los artículos 24 y 29 de la Ley». En sentido parecido, vid. la Consulta vinculante de la Dirección General de Tributos V0590-18, de 1 de marzo de 2018, que señala que «desde la perspectiva del Impuesto sobre el Patrimonio, habrán de declararse junto con el resto de los bienes, de la misma forma que se haría con un capital en divisas, valorándose en el impuesto a precio de mercado a la fecha del devengo, es decir, a 31 de diciembre de cada año» (en el mismo sentido la Consulta vinculante de la Dirección General de Tributos V2289-18, de 3 de agosto de 2018, respecto de la criptomoneda «iota»). Por otro lado, también es una cuestión controvertida si existe la obligación de efectuar la declaración del patrimonio en el extranjero, de acuerdo con el modelo 720, cuando el valor de las criptomonedas sea superior a 50.000 euros. De entrada, parece que no encaja en los supuestos contenidos en los artículos 42 *bis* y *ter* y 54 *bis* del Real Decreto 1065/2007, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos; motivo que exime de presentar tal declaración, máxime si se consideran como «otras órdenes de pago», como efectúa la Dirección General de Tributos. Ahora bien, en el caso de su posible asimilación, el problema vendría determinado por la consideración de qué sean bienes «en el extranjero». Sobre esta cuestión véase la nota n.º 91. Por otra parte, en el informe de 15 de febrero de 2017, elaborado por el Comisario europeo de Asuntos Económicos y Financieros, Fiscalidad y Aduanas, se apunta que tal y como está actualmente regulada, la declaración de bienes en el extranjero según el modelo 720 incumple varias de las libertades fundamentales de la Unión Europea, motivo por el cual solicita la modificación de la legislación. Ya en España, son varias las resoluciones judiciales que han aludido a la inadecuación de la normativa estatal con la regulación comunitaria en este punto. Por todas, vid. la STSJ de Castilla-León de 28 de noviembre de 2018 (JUR 2019, 20047).

[101] Efectuando un detallado análisis de por qué no resulta adecuada la conceptuación como «permuta», vid., VILARROIG MOYA, «Criptomonedas y otras clases de tokens: aspectos tributarios», en VV AA, *Blockchain: aspectos tecnológicos, empresariales y legales* –dirs. VILARROIG MOYA, R. y PASTOR SEMPERE, C.–, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 221-224.

## 6. LOS *SMART CONTRACTS* QUE SE EJECUTAN EN LA CADENA DE BLOQUES

Hasta ahora hemos examinado la cadena de bloques y hemos apuntado que en ella se pueden ejecutar los *smart contracts*. Es el momento de efectuar una breve explicación de este concepto. Aun cuando dicho término fue acuñado en la década de los noventa del pasado siglo por NICK SZABO utilizando como ejemplo una máquina expendedora, ha sido desde la aparición de la cadena de bloques cuando su presencia e importancia ha aumentado de manera considerable. Asimismo, el surgimiento de dicha «tecnología» permite distinguir entre los *smart contracts* que se verifican y ejecutan en una cadena de bloques y los que no están alojados ni se ejecutan en ella[102]. Ambos responden a una misma categoría conceptual –ambos son *smart contracts*– pero la «ubicación» en la cadena de bloques les dota de algunas características especiales –de una operativa específica– derivada del uso de dicha tecnología, a la vez que constituye el entorno natural para algunos de ellos –p. ej., los que transmiten criptoactivos–.

Desde una perspectiva técnica, el término *smart contract* alude únicamente a la secuencia de código informático que recoge las condiciones establecidas y las consecuencias que se desencadenarán de manera «automática» una vez se cumplan

[102] Hasta donde conocemos, el primero que hizo referencia a la dualidad a que se alude en el texto fue el jurista canadiense JOSH STARK («Making Sense of Blockchain Smart contracts», 4 de junio de 2016, https://bit.ly/2TnAtAU). De acuerdo con dicho autor, las características típicas de los *smart code contracts* serían: 1) que el programa en sí mismo se graba en *blockchain*, lo que le concede las características de permanencia y reluctancia a la censura propias de la cadena de bloques; 2) por sí mismo, el programa puede controlar *assets* de *blockchain* –por ejemplo, puede transferir una cantidad de criptomonedas–; y 3) el programa se ejecuta en la cadena de bloques, lo que significa que siempre se ejecutará como está escrito pues nadie puede interferir en él. Por otra parte, al no ser un objetivo específico de este artículo el análisis detallado de los «contratos inteligentes», nos remitimos a LEGERÉN-MOLINA, «Los contratos inteligentes en España (La disciplina de los *smart contracts*)», *Revista de Derecho civil*, vol. V, abril-junio, 2018, pp. 193-241, https://bit.ly/2H23P6O; trabajo que, aunque centrado en los *smart contracts* con relevancia jurídica que se ejecutan fuera de la cadena de bloques, analiza elementos también aplicables a los que tienen su acomodo en ella. En este sentido, una nota distintiva de aquellos en relación con estos reside en la necesidad que exista un ordenador que sea un «tercero imparcial» donde se ejecuten las secuencias de código. A este respecto, SONG («The truth about smart contracts», 11 de junio de 2018, https://bit.ly/2sO8e3k) señala que «that smart contract execution by a centralized party is not really trustless. You still have to trust the centralized party to execute. Trustlessness is the key feature, so centralized execution doesn't really make sense. To make smart contracts really trustless, you need a platform that's actually decentralized». De todas maneras, esta cuestión se analiza en el trabajo a que nos remitimos. Por último, recogiendo una definición de los «contratos inteligentes» en la cadena de bloques, vid., SAVELYEV, «Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law», 2017, DOI: 10.1080/13600834.2017.1301036, p. 12: «smart contract as a piece of software code, implemented on a Blockchain platform, which ensures self-performance and the autonomous nature of its terms, triggered by conditions defined in advance and applied to Blockchain-titled assets».

aquellas[103]. En tal sentido, cabe programar un *smart contract*, por ejemplo, tanto para transferir activos –operación con evidente trascendencia jurídica– como para construir un chat, desarrollar funciones de enlace telemático o procesos de comunicación en una aplicación; ejemplos últimos que, en sí mismos, carecen de relevancia jurídica alguna[104]. Ahora bien, desde otra perspectiva, esos comandos de código que son susceptibles de producir efectos jurídicos pueden integrarse o ser la expresión de un acuerdo existente entre las partes, motivo por el que los términos *smart contract* también se han utilizado –y así efectuamos en estas páginas– para aludir a tales acuerdos cuya peculiaridad esencial es que están escritos en código informático y son «autoejecutables»; es decir, en ellos la ejecución no depende de la voluntad de las partes, sino que, gracias a los comandos programados, tiene lugar de manera «automática», una vez se dan las condiciones preestablecidas por aquéllas. Para que ello pueda ocurrir, es preciso que las órdenes que las partes introduzcan en el código tengan lógica *booleana*; o, en otros términos, han de tener la estructura *if/then/else*: si se cumple esta circunstancia (*if*), entonces se ejecuta esta acción (*then*); de no cumplirse, se ejecuta otra acción también prevista (*else*). De esta manera, las obligaciones que, fruto del acuerdo, asumen las partes y que están contenidas o expresadas en el código, resultan claras y son verificables y «ejecutables» de manera «automática»[105].

[103] Aunque luego se señala de nuevo en el texto, conviene resaltar ahora que para que se produzca la ejecución –que denominamos «automática»– es preciso «llamar» o «activar» el *smart contract* que está alojado en la cadena de bloques; por este motivo, preferimos entrecomillar el referido «automatismo».

[104] En el mismo sentido, vid. IBAÑEZ JIMÉNEZ, *Derecho de blockchain y de la tecnología de registros distribuido*, cit., pp. 90 y 93. En efecto, a nuestro juicio, la terminología no ha de llevar a engaño pues que los *smart contracts* puedan producir efectos jurídicos, no significa que siempre y en todo caso ocurra así; hay *smart contracts* que no tienen tales efectos. Por tanto, bajo la indicada denominación caben los señalados en último lugar, así como los que producen efectos jurídicos, en los que el *smart contract* constituye un «soporte» para todo o parte de un acuerdo o contrato.

[105] Vid., a este respecto, las explicaciones sobre la terminología que se contienen en LEGERÉN-MOLINA, «Los contratos inteligentes en España (La disciplina de los *smart contracts*)», *cit.*, pp 195-200, del que transcribimos un párrafo en relación con el carácter «autoejecutable» a que se alude en el texto: «aun cuando señalamos que las máquinas «ejecutan una prestación escrita en el código», en sí mismos, los ordenadores «solamente» manejan datos y, actuando de acuerdo con unas reglas o algoritmos prefijados, producen otros resultados; en definitiva, procesan de manera automatizada datos según órdenes previamente establecidas. Al «producir» esos «nuevos datos» lo que, en realidad, están haciendo es «ejecutar» la prestación de que en cada caso se trate contenida en el acuerdo y de una manera automática» (*ídem*, p. 200). En definitiva, con el referido carácter autoejecutable se alude a que no es necesario que un tercero ejecute el contenido del acuerdo, pues los ordenadores, al procesar los datos de la manera programada, ya lo están haciendo por sí mismos. Desde el punto de vista informático, únicamente «se procesan datos»; pero tal proceso, examinado desde el prisma jurídico, constituye «el cumplimiento de una prestación» en aquellos *smart contracts* jurídicamente relevantes. En atención a lo que ahí se expone, se entiende que en ocasiones se afirme que «smart contracts were never intended to be legal contracts. NICK SZABO wanted to create new digital institutions» (SILLS, «The

Expuesto lo que antecede, ha de tenerse presente que constituyen minoría los *smart contracts* que no se acomodan en las cadenas de bloques, de manera que es usual identificar los «contratos inteligentes» con los que se ejecutan en ellas[106]. Lo anterior en parte se debe a que las cadenas de bloques hacen más viables y útiles los *smart contracts* –que ya existían con anterioridad– y cabe decir, «catapultan» a tal figura a un nuevo escenario[107]. En efecto, con la «tecnología» *blockchain* se han superado tres límites que entorpecían su desarrollo: la imposibilidad de hacer pagos programados y condicionados –lo que se resuelve con el uso de las criptomonedas, perfectamente programables–, la dificultad de que el código informático controle activos reales –lo que técnicamente se vence con la *tokenización*– y la inexistencia de ordenadores imparciales donde ejecutar el programa, aspecto que soluciona el carácter descentralizado de la cadena de bloques[108]. Asimismo, algunos de los inconvenientes que tradicionalmente suscitaban los contratos electrónicos –posibilidad de manipulación del mensaje, la prueba de su emisión y recepción, etc.–, además de atajarse por ciertos medios ya utilizados –los protocolos de seguridad existentes o la misma firma electrónica– se resolverán también, y de manera eficaz, por medio de la

forgotten contracts», 5 de junio de 2018, https://bit.ly/2I4S9Ci), como que se examine en detalle las normas jurídicas que le resultan de aplicación a los acuerdos que se implementan mediante código informático (TUR FAÚNDEZ, *Smart Contracts. Análisis jurídico*, cit., pp. 63 y ss.). Finalmente, respecto del carácter «inteligente» o no de los «contratos» a que aludimos, vid. LEGERÉN-MOLINA, «Los contratos inteligentes en España (La disciplina de los *smart contracts*)», *cit.*, pp. 211 y ss., SONG, «The truth about smart contracts», *cit.*, quien señala que «a truly intelligent contract would take into account all the extenuating circumstances, look at the spirit of the contract and make rulings that are fair even in the most murky of circumstances. In other words, a truly smart contract would act like a really good judge. Instead, a «smart contract» in this context is not intelligent at all», y, finalmente, lo que VITALIK BUTERIN indicaba en su cuenta de twitter el 13 de octubre de 2018: «to be clear, at this point I quite regret adopting the term *smart contracts*. I should have called them something more boring and technical, perhaps something like *persistent scripts*».

[106] Tal y como apunta ECHEBARRÍA SÁENZ («Contratos electrónicos autoejecutables…», *cit.*, pp. 70, 75 y 80) la general identificación de los «contratos inteligentes» con los que se efectúan en una cadena de bloques se debe, fundamentalmente, a dos razones. De un lado, a que abundan las plataformas que promueven este modelo de contratos usando la referida tecnología. Y, de otro, a que las cadenas de bloques sí permiten programar pagos sin necesidad de intervención humana posterior que los ordene; lo que no ocurre con los sistemas de pago a distancia actualmente ofertados por las entidades de crédito –aunque podrían implementar un sistema que lo permitiese–.

[107] En sentido similar, vid., BELLAMY y HILL, «Can the Blockchain Make Our Contracts Smarter?», 21 num. 11, *Cyberspace Lawyer NL 2*, December, 2016, o BUTLER, AL KHALIL, CECI y O'BRIEN, «Smart contracts and distributed ledger technologies in financial services: keeping layers in the loop», 36 num. 9 *Banking & Financial Services Policy Report* 1, September, 2017, p. 2. Y, manteniendo una opinión parecida, pero haciendo específica referencia a las criptomonedas, vid., KOST DE SEVRES, CHILTON y COHEN, «The Blockchain Revolution, Smart contracts and Financial Transactions», 21 num. 5 *Cyberspace Lawyer NL* 3, June, 2016, p. 3.

[108] Igualmente, los «contratos inteligentes» ofrecen una vía para mitigar el problema de la confianza respecto de la actitud de la otra parte para ejecutar o no el contrato. Sobre la problemática relativa a la eficacia que se le conceda fuera del mundo virtual a los bienes «tokenizados», vid. la nota n.º 4.

utilización de la «tecnología» *blockchain*[109]. En consecuencia, los *smart contracts* ejecutados en la cadena de bloques se benefician del sellado de tiempo, del carácter inmutable, de la reducción de costes y de la mayor eficacia propias de aquella[110], así como de las ventajas específicas de todo «contrato inteligente» con relevancia jurídica derivadas de ser «autoejecutables» y de su carácter objetivo, que les dota de seguridad al desterrar ambigüedades y reducir o eliminar eventuales problemas de interpretación del acuerdo[111]. De lo anterior también se colige que será innecesaria la intervención de un tercero que supervise la ejecución de los acuerdos a que nos referimos: son las propias máquinas las que, verificando de manera objetiva que concurren las condiciones predeterminadas, ejecutan lo establecido para tal evento[112]. De todos modos, no ha de olvidarse que una vez se programe un *smart contract*, ha de «publicarse» (*deploy*) en una cadena de bloques, tras lo cual es preciso «llamar» al *smart contract* para ejecutarlo (*call*) –ejecución que goza de carácter automático e «inexorable»–, sin que sea infrecuente que se establezca un mecanismo para su paralización (*suicide*).

Ahora bien, el hecho de que el «contrato inteligente» se ejecute en la cadena de bloques no le priva de sus límites intrínsecos: por las exigencias propias del lenguaje del

[109] Evidentemente, la figura a que ahora se alude origina otras cuestiones: *ad ex*. el foro ante el que resolver los eventuales litigios. En este punto, ha de tenerse presente que los interrogantes que suscitan los *smart contracts*, en parte son distintos si están alojados en cadenas de bloques públicas –Ethereum, NXT, etc.– o privadas –donde destacan las del consorcio Hyperledger (Hyperledger Burrow, Hyperledger Fabric…) o, fuera de él, Quorum, entre otras–. Finalmente, sobre la relación de los *smart contracts* con el Reglamento Europeo de Protección de Datos, vid., FINCK, «Smart Contracts as a Form of Solely Automated Processing Under the GDPR», *Max Planck Institute for Innovation & Competition Research Paper* n. 19-01, 8 de enero de 2019, disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370.

[110] Cfr. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 3. La innecesariedad de elementos humanos para la verificación de las condiciones establecidas en el contrato, por ejemplo, les dota de mayor rapidez en la ejecución, a la vez que elimina la posibilidad de errores cometidos por las partes.

[111] Cfr. BELLAMY y HILL, «Can the Blockchain Make Our Contracts Smarter?», *cit*. Respecto de la eliminación de los términos ambiguos, vid. KOST DE SEVRES, CHILTON y COHEN, «The Blockchain Revolution, Smart contracts and Financial Transactions», *cit.*, p. 3; y en sentido parecido, BUTLER, AL KHALIL, CECI y O'BRIEN, «Smart contracts and distributed ledger technologies in financial services…», *cit.*, p. 2. De otra parte, mencionando la escalabilidad del sistema, con su consiguiente aumento de valor y de dificultad de comprometerlo, vid. FAIRFIELD, «Smart contract, bitcoin, bots and consumer protection», *cit.*, p. 40; y SHERIDAN, «Bitcoins: Currency of the Geeks», 16 de junio de 2011, https://bloom.bg/2F7ztgz. En consecuencia, las posibilidades que ofrecen los «contratos inteligentes» son amplias pues podrán ser usados en gran variedad de ámbitos, aun cuando actualmente aun se apliquen «poco» (cfr. MCJOHN y MCJOHN, «The Commercial Law of Bitcoin and Blockchain Transactions», *cit.*).

[112] La posibilidad de entablar transacciones de confianza es una de las características más importantes de la cadena de bloques en relación a los «contratos inteligentes»; cfr. KOST DE SEVRES, CHILTON y COHEN, «The Blockchain Revolution, Smart contracts and Financial Transactions», *cit.*, p. 3. En el mismo sentido vid. BRIDGERS, «Will workplaces be going off the rails on the blockchain?», *cit.*, p. 3.

código y su lógica *booleana*, seguirán siendo una herramienta útil únicamente para el amplio espectro de acuerdos que sean objetivables y permitan su autoejecución –p. ej. en contratos de suministro o pagos–[113]. En consecuencia, este tipo de contratos no admite cláusulas que necesiten de interpretación para ser verificadas –buena fe, consumidor medio, diligencia debida, etc.–, ni tampoco tienen perfecta cabida en ellos conceptos como «caso fortuito» o «fuerza mayor» (cfr. art. 1105 CC)[114]. Así las cosas, ha de tenerse en cuenta que la ventaja señalada –la ejecución automática una vez «activado» el *smart contract*, que constituye, en cierto sentido, una autoprotección de los contratantes– puede ser también un inconveniente ya que no admite modulaciones en su ejecución o renegociaciones o acuerdos adecuados al desarrollo de los eventos.

Cuando los *smart contracts* con relevancia jurídica se ejecutan en una cadena de bloques pública un problema básico es la determinación de los criterios legales que le resultan de aplicación. Cierto es que la idea con que surgieron estas cadenas era establecer un sistema de pagos alternativo al vigente –eliminando la necesidad de intermediarios– al ser una base de datos descentralizada y permanente y, en cierta medida, que «actúa fuera de las fronteras del Derecho». Pero cierto es también que cuando surjan problemas en la ejecución –*bugs* en el código, por ejemplo–, ha de arbitrarse algún sistema de reclamación; dificultad que se agrava por el hecho de que en las cadenas de bloques intervienen personas de diferentes jurisdicciones. En tal sentido, y como ya se ha mencionado, en algunos Estados se está desarrollando legislación tanto sobre las cadenas de bloques como sobre los *smart contract*.

[113] «As a cryptocurrency technology platform, *Bitcoin* is capable of executing *smart contracts*, but with noteworthy restrictions due to its limited scripting language» (BUTLER, AL KHALIL, CECI y O'BRIEN, «Smart contracts and distributed ledger technologies in financial services…», *cit.*, p. 2). Así las cosas, en parte la limitación del lenguaje de *Blockchain* ha dado lugar al desarrollo de la ya mencionada Ethereum: plataforma descentralizada donde los «contratos inteligentes» tienen perfecto acomodo pues está equipada con un completo lenguaje de programación acorde con el test de Turing. Recientemente, también han sido desarrolladas otras plataformas que permiten *smart contracts* con el referido lenguaje –a modo de ejemplo cabe mencionar Rootstock– y otras sin él.

[114] Cfr. WERBACH y CORNELL, «Contracts *ex machina*», *Duke Law Journal*, 67, 2017, p. 367, y PRENAFETA RODRÍGUEZ, «*Smart contracts*: aproximación al concepto y problemática legal básica», *Diario La Ley*, nº 8824, 15 de septiembre de 2016. En sentido similar, SAVELYEV («Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law», *cit.*, p. 10) señala que «a computer language does not allow discretion in its interpretation by the machine. *Smart contract* terms are interpreted by machine on the basis of *Boolean* logic, in contrast to classic contracts, where interpretation of terms is performed by the human brain on the basis of subjective criteria and analogous ways of thinking». Por lo expuesto en el texto, los *smart contracts* resultan más frecuentes en el ámbito de los contratos de suministro, la fabricación de productos, o el intercambio de bienes por dinero, entre otros. Si, como se prevé, el denominado «internet de las cosas» –*internet of things* (*IoT*)– se expandirá en un futuro próximo de manera que el número de dispositivos conectados y que «emitan» información se multiplique exponencialmente –afectando, por ejemplo, a elementos domésticos de viviendas inteligentes como cañerías, electrodomésticos, etc.–, el ámbito de los «contratos inteligentes» crecerá.

Con todo, lo idóneo es que, si las partes han formalizado el acuerdo que han volcado total o parcialmente en un *smart contract* liberándose así de «ejecutar personalmente las prestaciones», hayan determinado los criterios legales para la resolución de controversias. En cualquier caso, y al igual que sucedía respecto de la cadena de bloques, en España no existe una legislación específica relativa a los acuerdos susceptibles de producir efectos jurídicos que están escritos en código informático y que se ejecutan usando la referida tecnología. Por tal motivo, ha de acudirse entonces a la normativa general de los negocios jurídicos y contratos, a la que regula la contratación electrónica y a la relativa a los servicios de la información, a pesar de que no den respuesta acabada a todos los eventuales problemas. Lo anterior es posible porque, aun cuando si nos ceñimos únicamente a la perspectiva técnica –la secuencia de código– los *smart contracts* no sean en sí mismos un contrato, tal código puede expresar o formar parte de un acuerdo con relevancia jurídica que le da sentido, que sí puede ser conceptuado como una modalidad de los contratos electrónicos, constituyendo entonces el código el soporte de éste. A tales acuerdos –implementados o expresados total o parcialmente por medio del código– les resultará entonces de aplicación el artículo 23 de la Ley de Servicios a la Sociedad de la Información que remite al Código civil y de Comercio para los requisitos necesarios para su validez[115]. En consecuencia, tales acuerdos habrán de reunir los requisitos básicos de cualquier contrato: «*objeto cierto que sea materia del contrato*» (art. 1261 CC), la «*causa de la obligación que se establezca*» (art 1261 CC) y el consentimiento, que puede emitirse de manera oral, escrita, o a través de medios informáticos.

Cuando los «contratos inteligentes» se elaboren para ser suscritos en serie y dirigidos a consumidores también resultará de aplicación la normativa específica[116]. En concreto, el régimen jurídico de las cláusulas generales de los contratos celebrados con consumidores (cfr. *ad ex.*, arts. 5 a 10 de la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación), el relativo a las cláusulas no negociadas individualmente (cfr. arts. 80-91 del RD Legislativo 1/2007, de 16 de noviembre, de Texto Refundido de la Ley General de la Defensa de Consumidores y Usuarios), las disposiciones atinentes a la información precontractual y postcontractual (cfr. *ad ex.* arts. 27 y 28 LSSI y el art. 98

[115] En concreto, el artículo 23 de la LSSI dispone que «*los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez. Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial*».

[116] Reconociendo que, por su estructura igualitaria, los «contratos inteligentes» no protegen a las partes débiles –p. ej. consumidores–, vid. SAVELYEV, «Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law», *cit.*, p. 16.

TRLGDCU) y la exigencia de entregar al consumidor una copia del contrato impresa o en soporte duradero, de manera que cuando haya divergencia entre el contenido del código informático y la versión entregada a aquél, prevalecerá ésta (*arg. ex* arts. 61, 63, 65, 80, 98 y 99 TRLGDCU, entre otros).

Así las cosas, otro de los aspectos característicos de los *smart contracts* que se ejecutan en una cadena de bloques se refiere al «cumplimiento del acuerdo» y consiste en que el pago está automatizado. Ello facilita que se produzca el triple efecto que comúnmente se le reconoce al pago: extintivo, liberatorio y satisfactivo. Asimismo, al estar establecida la ejecución de la prestación con carácter «automático», tendencialmente no tendrá lugar el incumplimiento –aunque de hecho pueda ocurrir– [117]. Los «contratos inteligentes» no hacen más sencilla la ejecución; en cierto sentido, cabe decir, la hacen inevitable[118].

Por otra parte, el hecho de que el *smart contract* se ejecute en la cadena de bloques no modifica el criterio general respecto del «lugar de cumplimiento» de la obligación pues ha de entenderse que el pago efectuado *en ella* es el resultado de un acuerdo de las partes, ya expreso, ya tácito (cfr. art. 1171 CC), que se implementa en la secuencia de código informático. Y en lo relativo al recibo como prueba del cumplimiento, a nuestro juicio, el sellado de tiempo propio de la cadena valdrá como prueba de la realización de la prestación –evidentemente, con la fuerza probatoria de un documento privado–[119].

[117] Hasta tal punto ello es así que ECHEBARRÍA SÁENZ («Contratos electrónicos autoejecutables…», *cit.*, p. 73) ha señalado que, en atención a que la ejecución en este tipo de contratos es la respuesta automática ante un evento prefijado por las partes, «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 éste no se haya consagrado en nuestro sistema legal. En consecuencia, negada la mayor, no constituye un problema negar la menor; esto es, la «renuncia» a la *exceptio non adimpleti contractus*.

[118] Cfr. WERBACH y CORNELL, «Contracts *ex machina*», *cit.,* p. 348, donde también afirman que «in order to do so, they change the nature of the contract itself». La parte negativa de este automatismo –como ya hemos señalado– es la imposibilidad de parar la ejecución de un contrato que resulte inadecuado (en el mismo sentido, *ídem*, p. 373).

[119] Asimismo, el carácter automático del pago dificulta el realizado por tercero –no tiene mucho sentido que alguien se ofrezca a pagar, siendo aquel «automático»; existirá posiblemente un doble pago que tendrá carácter inmutable–. Igualmente, también impide los subrogados del cumplimiento pues el código informático está pensado para ejecutar y realizar la prestación pactada por las partes de manera exacta. Razón por la cual tampoco parecen viables otros elementos clásicos relacionados con el pago como son la consignación, el ofrecimiento del pago, o la imputación de pagos. En este último caso, la cadena de bloques únicamente valdrá como registro de que se ha efectuado una transacción. Será la contabilidad que lleven acreedor y deudor los que determinen a qué deuda se imputa, aun cuando el carácter «automático» del *smart contract* minimiza los casos donde se proceda a tal imputación.

Ahora bien, aunque los *smart contract* sean piezas de código que, una vez se «activen», se ejecutan «automáticamente», facilitando, de entrada, la inexistencia de errores, tales disfunciones existen; especialmente cuando se clonan «contratos inteligentes»[120]. A modo de ejemplo, ello puede ocurrir porque no se haya codificado de manera adecuada lo que las partes pretendían con el *smart contract* –lo que requiere una adecuada conjunción de juristas y programadores–, porque la escritura en código tenga algún *bug* –a fin de evitarlos, es muy recomendable una auditoría sobre el código realizada por técnicos que no hayan hecho el desarrollo en sí del *smart contract*–, porque la plataforma interpreta el código de manera distinta a cómo previeron los programadores, porque falle la plataforma en que se alojan –p. ej. se produce un ataque a la cadena–, porque una de las partes retira los criptoactivos de la cuenta desde donde habrían de transferirse, porque un tercero «hackea» el código o los oráculos e impide la ejecución; por mal funcionamiento de los nodos, etc. En tales supuestos y aun cuando existen mecanismos «arbitrales» dentro de las cadenas para la resolución de conflictos, es preciso buscar soluciones, así como criterios de imputación de la responsabilidad que corresponda. Y a tal fin, habrá que ver cómo son «aceptados» y reconocida su coercibilidad por los tribunales de justicia. De entrada, a lo que parece, como meros acuerdos de carácter privado pues su inclusión en una cadena de bloques no los convierte, en modo alguno, en un documento público.

Como se advierte, con la normativa actual se puede dar solución a algunas de las cuestiones que suscitan los *smart contract* aun cuando parece que habrá que ir adaptándola para dar respuesta a otras que actualmente no encuentran fácil acomodo. En tal sentido, parece que las disposiciones legales que se dicten en el futuro habrán de incidir en la protección a los consumidores –garantizando la validez del consentimiento que prestan–, habrán de buscar sistemas de arbitraje y de coercibilidad fuera de la cadena, o, en fin, habrán de desarrollar la escasa normativa actual sobre tratos preliminares y oferta contractual para adaptarla a las cadenas de bloques.

## 7. CONCLUSIONES

De entre las numerosas conclusiones que cabría extraer de los análisis realizados a lo largo del presente trabajo, a continuación, enunciaremos de manera sintética solamente algunas, por parecernos las más significativas.

En primer lugar, de lo expuesto en las páginas precedentes se adivina que, en lo que hace al uso de la «tecnología» *blockchain*, aun estamos en los primeros estadios. Así, y

[120] En tal sentido, vid. la investigación desarrollada entre la Universidad de Northeastern y la Universidad de Maryland (USA) en https://mislove.org/publications/Ethereum-IMC.pdf.

aunque actualmente sean muchos los proyectos que intentan utilizar la cadena de bloques, no serán tantos los que finalmente cristalicen y se consoliden. Ello se debe, entre otros motivos, a que el resultado que han de arrojar habrá de –eliminando los «intermediarios innecesarios»– satisfacer las necesidades existentes con el mismo grado de seguridad y a un menor costo; requisitos no sencillos de cumplir. En tal sentido, sí parece que reúne tales características y arraiga el uso de *blockchain* como plataforma para la realización de pagos –utilizando para ello *smart contracts*–; aspecto que –se reconozca o no en el futuro a las criptomonedas como dinero legal y no sólo como medio de pago– mejorará en cuanto se atempere la volatilidad de aquellas, propiciada, en buena medida, por la actividad especulativa. El referido afianzamiento en parte se debe a que, al realizarse tales operaciones totalmente *on-chain*, se minimizan las posibles «brechas» que podrían hacer inútil el uso de la cadena de bloques. En muchas de tales transferencias toda la información necesaria está *on-chain*, de modo que no resulta necesario depender de oráculos externos o del *Internet de las cosas* (*IoT*) que, en lo que ahora interesa, aún no proporciona un elevado nivel de seguridad en la verificación, al poder ser objeto de manipulación.

Igualmente, en los próximos años, junto con las cadenas públicas actualmente existentes, seguirán creciendo otras de carácter privado que, aun cuando «contradigan» el propósito con que originariamente se concibió *Blockchain*, aprovecharán esta «nueva filosofía» o «nuevo modo de hacer». Una ventaja de este tipo de cadenas es la mayor libertad que ofrecen para su configuración, pudiendo, por ello, diseñarse desde el inicio para que susciten menos dificultades desde la perspectiva legal: cabe configurarlas de manera que sean *GDPR-compliant*, señalando claramente la normativa que resulte aplicable, etc. Con todo, las diversas autoridades también irán aprobando legislaciones a fin de regular y resolver las cuestiones que suscita la cadena de bloques, ya sean privadas, ya sean públicas: *ad ex.*, su valor en un proceso, el modo de tributar, cómo evitar su uso para el blanqueo de capitales o el foro que resulte de aplicación.

Sea ello como fuere, en cualquier caso, entiendo que las cadenas de bloques no reemplazarán ni la función notarial ni los Registros de derechos, tal y como están concebidos en España. Ninguno de ellos constituye un intermediario «innecesario». En efecto, ambos aportan valor con el control jurídico y de legalidad que realizan respecto de la transacción que se pretende efectuar, con el análisis de la capacidad o el consentimiento de las partes, o, en fin, porque acreditan el reconocimiento por parte del Estado de la titularidad de los derechos registrados, generando confianza en los operadores económicos. Cuestión distinta es que se recurra a *blockchain* como «herramienta tecnológica» para algunas funciones de mera «notarización» o

«registro», aun cuando existan actualmente otros modos de conseguir efectos similares –p. ej. por el sellado de tiempo–. Pero, en todo caso, el recurso a las cadenas de bloques será como instrumento «accesorio» y no en el sentido «sustantivo» apuntado, una vez se demuestre que su uso garantiza la misma seguridad y eficiencia y a un menor coste.

BIBLIOGRAFÍA.

ANGUIANO, J.M., «*Blockchain*: fundamentos y perspectiva jurídica. De la confianza al consenso», *Diario La Ley*, nº 18, 16 de mayo de 2018.

ARRUÑADA, B., «Blockchain in Public Registries: Don't Expect Too Much», *IPRA Cinder International Review*, nº 1, January-June, 2017, pp. 6-11.

— «Blockchain's Struggle to Deliver Impersonal Exchange», *Minnesota Journal of Law, Science & Technology*, vol. 19, 2018, pp. 55 y ss.

— «Limitaciones de *blockchain* en contratos y propiedad», *Revista Crítica de Derecho Inmobiliario*, nº 769, 2018, pp. 2465 a 2493.

BACON, J., MICHELS, J. D., MILLARD, C., SINGH J., «Blockchain demystified: a technical legal introduction to distributed and centralized ledgers», *Richmond Journal of Law & Technology,* volume 25, issue 1, 2018, pp. 1-106.

BELL, T. W., «Copyrights, Privacy, And The Blockchain», 42 *Ohio Northern University Law Review* 439, 2016.

BELLAMY, J. y HILL C., «Can the Blockchain Make Our Contracts Smarter?», 21 num. 11, *Cyberspace Lawyer NL 2*, December, 2016.

BODÓ, B., GERVAIS, D. y QUINTAIS, J. P., «Blockchain and smart contracts: the missing link in copyright licensing?», *International Journal of Law and Information Technology*, volume 26, Issue 4, 1 December 2018, pp. 311–336, https://doi.org/10.1093/ijlit/eay014

BRANCÓS, E., «*Blockchain*, función notarial y registro», https://bit.ly/2TpxxUA

— «El papel del notario y el *Blockchain*», *Escritura Pública*, nº 106, julio-agosto, 2017.

BRIDGERS, A., «Will workplaces be going off the rails on the blockchain?», *20 num. 11 Journal of Internet Law* 3, May, 2017.

BUTERIN, V., «The meaning of decentralization», 6 de febrero de 2017, https://bit.ly/2tEUYyT

BUTLER, T., AL KHALIL, F., CECI, M., y O'BRIEN, L., «Smart contracts and distributed ledger technologies in financial services: keeping layers in the loop», 36 num. 9 *Banking & Financial Services Policy Report* 1, September, 2017.

CARRASCOSA COBOS, C., «Cryptocurrencies may finish with tax systems as we know them», 4 de febrero de 2018, https://bit.ly/2CiZQOd

COMITÉ SOBRE LAS LIBERTADES CIVILES, JUSTICIA Y ASUNTOS INTERNOS del Parlamento Europeo, «Opinión sobre *blockchain*» (2018/2085(INI)) al Comité de Transacciones Internacionales, de 15 de noviembre de 2018, disponible en https://bit.ly/2Rxr6RK.

DÍEZ GARCÍA, D. y GÓMEZ LARDIES, G., «Banca y *blockchain*, ¿pioneros por necesidad?», en VV AA, *Blockchain: la revolución industrial de internet* –coord. PREUKSCHAT, A.–, Gestión 2000, Barcelona, 2017, pp. 32-42.

DUIVESTEIN, S. y SAVALLE, P., «Bitcoin: It's the platform, not the currency, stupid!», 15 de febrero de 2014, https://bit.ly/2VsFOsA.

ECHEBARRÍA SÁENZ, M., «Contratos electrónicos autoejecutables (*smart contract*) y pagos con tecnología *blockchain*», *Revista de Estudios Europeos*, nº 70, julio-diciembre, 2017, pp. 69-97.

EUROPEAN CENTRAL BANK, *Virtual currency schemes*, october 2012, disponible en la web http://www.ecb.europa.eu en el apartado de *Research & Publications*.

FAIRFIELD, J., «Smart contract, bitcoin, bots and consumer protection», *71 Washington and Lee Law Review Online* 35, September, 2014.

FARMER, Jr., «Speculative Tech: The Bitcoin Legal Quagmire and the Need for Legal Innovation», *9 Journal of Business & Technology Law* 85, 2014.

FINCK, M., «Blockchain regulation» (August 7, 2017), *German Law Journal*, 2018, *Max Planck Institute for Innovation & Competition Research Paper* nº 17-13, disponible en SSRN: https://ssrn.com/abstract=3014641 or http://dx.doi.org/10.2139/ssrn.3014641

— «Smart Contracts as a Form of Solely Automated Processing Under the GDPR», *Max Planck Institute for Innovation & Competition Research Paper* n. 19-01, 8 de enero de 2019, disponible en SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370

FINANCIAL ACTION TASK FORCE (FATF), «Virtual currencies – key definitions and potential AML/CFT risks», June, 2014, https://bit.ly/1CXF0dj

FRIDMAN, A., *How to design a GDPR-compliant blockchain*, 23 de mayo de 2018, https://bit.ly/2GON49D

GALLEGO FERNÁNDEZ, L. A., «Blockchains and Title Registration», *IPRA Cinder International Review*, nº 1, January-June, 2017, pp. 26-51.

— «Cadenas de bloques y Registros de derechos», *Revista Crítica de Derecho Inmobiliario*, nº 765, enero-febrero, 2018, pp. 97-141.

GOMÁ GARCÉS, I., «La transmisión de la propiedad de *Bitcoin*», 28 de junio de 2015, https://bit.ly/2F6vmkU

GONZÁLEZ GRANADO, J., «Sólo se muere una vez: ¿Herencia digital?», 23 de diciembre de 2015, https://bit.ly/2F5elaB

— «Eficacia probatoria de la *blockchain*. Criptografía y artículo 1227 del Código Civil», 25 de abril de 2016, https://bit.ly/2LQHsQ8

— *Retos del BitCoin y de la Blockchain*, en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 129-143.

GONZÁLEZ-MENESES, M., *Entender blockchain. Una introducción a la tecnología de registro distribuido*, Thomson Reuters Aranzadi, Cizur Menor, 2017.

— «La reflexión pendiente sobre *blockchain*», https://bit.ly/2Tos4Ny, 14 de marzo de 2018.

HUGHES, S. J., y MIDDLEBROOK, S. T., «Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries», 32 *Yale Journal on Regulation*, 495, 2015.

IBAÑEZ JIMÉNEZ, J. W., *Derecho de blockchain y de la tecnología de registros distribuido*, Thomson Reuters Aranzadi, Cizur Menor, 2018.

— Informe sobre monedas virtuales (2016/2007(INI)) de la Comisión de Asuntos Económicos y Monetarios del Parlamento europeo, https://bit.ly/2CNzfcI

IVANITSKIY, I., «You Do Not Need Blockchain: Eight Popular Use Cases And Why They Do Not Work», 22 de febrero de 2019, https://bit.ly/2GXjLFC

JOHNSON, G. L., «Planning the future, Blockchain Technology and the Insurance Industry», 12 num. 4 *In-House Defense Quarterly* 73, fall, 2017.

KAAL, W., «Initial Coin Offerings: the top 25 jurisdictions and their comparative regulatory responses», 3 de febrero de 2018, https://bit.ly/2nM75WG

KAAL, W. y CALCATERRA, C., «Crypto transaction dispute resolution», *The Business Laywer*, Spring 2018.

KEMP, R., «Legal Aspects of Artificial Intelligence», 22 num. 1 *Cyberspace Lawyer NL* 2, January February, 2017.

KOST DE SEVRES, N., CHILTON, B. y COHEN, B., «The Blockchain Revolution, Smart contracts and Financial Transactions», 21 num. 5 *Cyberspace Lawyer NL* 3, June, 2016.

LASKOWSKI, M., «A Blockchain-Enabled Participatory Decision Support Framework», en VV AA, *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*, Springer, Cham, 2017, pp. 329-334.

LEGERÉN-MOLINA, A., «Los contratos inteligentes en España (La disciplina de los *smart contracts*)», *Revista de Derecho civil*, vol. V, abril-junio, 2018, pp. 193-241, https://bit.ly/2H23P6O

LLOPIS BENLLOCH, J. C., «*Blockchain* y profesión notarial», https://bit.ly/2RpHa8k

— «Herencias con *bitcoin*, un caso de futuro», 31 de julio de 2014, https://bit.ly/2K78EI4

— «*Bitcoin* como medio de pago en la compra de bienes», 19 de diciembre de 2017, https://bit.ly/2Jv0YmL

— *El notario ante la identidad y la capacidad digital*, en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 181-189.

MASSACCI, F., NGO, Ch.-N. y WILLIAMS, J., «Decentralized Transaction Clearing Beyond Blockchains», (June 13, 2016), Technical report SSRN 2794913, disponible en http://dx.doi.org/10.2139/ssrn.2794913

MCJOHN, S. y MCJOHN, I., «The Commercial Law of Bitcoin and Blockchain Transactions», 47 num. 2 *Uniform Commercial Code Law Journal ART 4*, July, 2017.

MORA, «Las ICOs no están reguladas… ¿o sí? Análisis jurídico de la token-economía», 13 de octubre de 2018, https://bit.ly/2BYMHJi.

NAKAMOTO, S., «Bitcoin: A Peer-to-Peer Electronic Cash System», https://bitcoin.org/bitcoin.pdf

NARAYANAN, A., BONNEAU, J., FELTEN, E., MILLER, A. y GOLDFEDER, S., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, 2016.

O'SHIELDS, R., «Smart contracts. Legal agreements for the blockchain», 21 *North Carolina Banking Institute* 177, March, 2017.

OTERO MOREIRAS, I., «Los tokens vistos por un abogado», 11 de octubre de 2017, https://bit.ly/2VrAB4j.

PACHECO JIMÉNEZ, Mª N. y SALES PALLARÉS, L., «Los medios de pago en el escenario virtual: el dinero electrónico y el *bitcoin*», en VV AA, *Derecho digital: retos y cuestiones actuales*, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 145-160.

— Plan de acción del Parlamento Europeo y del Consejo para fortalecer la lucha contra la financiación del terrorismo (*Action Plan for strengthening the fight against terrorist financing*, Strasbourg, 2.2.2016 COM (2016) 50 final).

PRENAFETA RODRÍGUEZ, J., «*Smart contracts*: aproximación al concepto y problemática legal básica», *Diario La Ley*, nº 8824, 15 de septiembre de 2016.

PREUKSCHAT, A., «Los fundamentos de la tecnología *blockchain*», en VV AA, *Blockchain: la revolución industrial de internet* –coord. PREUKSCHAT, A.–, Gestión 2000, Barcelona, 2017, pp. 23-30.

RAMOS MEDINA, I., «Propiedad intelectual, notarios y *blockchain*», 7 de diciembre de 2016, https://bit.ly/2h2GyAs

RAMOS SUÁREZ, F. Mª, «La prevención del blanqueo de capitales y el *Bitcoin*», 18 de septiembre de 2015, https://bit.ly/2C0oS3w

SAVELYEV, A., «Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law», *Information & Communications Technology Law*, 2017, DOI: 10.1080/13600834.2017.1301036, pp. 1-19.

SCHNEIER, B., «There's no good reason to trust blockchain technology», 6 de febrero de 2019, https://bit.ly/2WKlRy6

SHERIDAN, B., «Bitcoins: Currency of the Geeks», 16 de junio de 2011, https://bloom.bg/2F7ztgz

SILLS, K., «The forgotten contracts», 5 de junio de 2018, https://bit.ly/2l4S9Ci

STARK, J., «Making Sense of Blockchain Smart contracts», 4 de junio de 2016, https://bit.ly/2TnAtAU

STINCHCOMBE, «Ten years in, nobody has come up with a use for blockchain», 22 de diciembre de 2017, https://bit.ly/2zqiRKj

STRICK, B., «Tracing an offshore bank and a dark web service using the blockchain — an OSINT investigation», 6 de septiembre de 2018, https://bit.ly/2Ho0cGN

SOLEY, J., «Cómo cambiará *blockchain* tu manera de hacer pagos», *IESEinsight*, nº 35, septiembre-diciembre, 2017, pp. 47-52.

SONG, J., «The truth about smart contracts», 11 de junio de 2018, https://bit.ly/2sO8e3k

TAPSCOTT, D. & TAPSCOTT, A., *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, Penguin Random House, 2016.

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, «Scalability, interoperability and sustainability of blockchains», 6 de marzo de 2019, disponible en https://bit.ly/2EZhgQl

— «Blockchain and the GDPR», 16 de octubre de 2018, disponible en https://www.eublockchainforum.eu/reports

TINIANOW, A., «Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance», 16 de marzo de 2017, https://bit.ly/2Syeozv

TSUKERMAN, M., «The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions For The Future», 30 *Berkeley Technology Law Journal* 1127, 2015.

TUR FAÚNDEZ, C., *Smart Contracts. Análisis jurídico*, Reus, Madrid, 2018.

UNIFORM LAW COMMISSION UNIFORM REGULATION OF VIRTUAL CURRENCY BUSINESSES ACT, https://bit.ly/2VssAw3

VILARROIG MOYA, R., «Criptomonedas y otras clases de tokens: aspectos tributarios», en VV AA, *Blockchain: aspectos tecnológicos, empresariales y legales* –dirs. VILARROIG MOYA, R. y PASTOR SEMPERE, C.–, Thomson Reuters Aranzadi, Cizur Menor, 2018, pp. 191-241.

VV AA, *Blockchain: la revolución industrial de internet* –coord. PREUKSCHAT, A.–, Gestión 2000, Barcelona, 2017.

— *Criptoderecho. La regulación de Blockchain* –dir. GARCÍA MEXÍA–, La Ley-Wolters Kluwer, Madrid. 2018.

WALL, E., «Privacy and Cryptocurrency, Part I: How Private is Bitcoin?», 7 de marzo de 2019, https://bit.ly/2EL7lxX

WERBACH, K. y CORNELL, N., «Contracts *ex machina*», *Duke Law Journal*, 67, 2017, pp. 313-382.

WIRDUM, A. v., «Keep an eye out for these bitcoin tech trends in 2018», 2 de enero de 2018, https://bit.ly/2E4xNAp

Fecha de recepción: 19.07.2018

Fecha de aceptación: 02.04.2018