TECNOLOGÍA *BLOCKCHAIN*: FUNCIONAMIENTO, APLICACIONES Y RETOS JURÍDICOS RELACIONADOS

Núria Porxas y Maria Conejero
*Abogadas**

Tecnología *blockchain:* funcionamiento, aplicaciones y retos jurídicos relacionados

La tecnología blockchain es una de las tecnologías sobre las que más se ha debatido en los últimos meses. Aunque su aplicación más popular son las llamadas "criptomonedas" o "criptoactivos", existen muchos otros campos en los que se están considerando, y ya realizando, usos de esta tecnología. El trabajo presenta brevemente las claves para poder entender y valorar su potencial: repasa los fundamentos de su funcionamiento, describe sus aplicaciones, y apunta, en fin, algunos retos jurídicos que su utilización plantea.

Palabras clave
blockchain, redes descentralizadas

Blockchain *technology:* workings, applications and related legal challenges

Blockchain technology has been one of the most debated technologies in recent months. While cryptocurrencies or cryptoassets are among its most popular applications, there are many other fields in which the use of this technology is being considered or is already being implemented. This article presents the keys to understanding and assessing its potential, by offering an overview of the basics of how it works, describing its applications and pointing out some of the legal challenges they pose.

Key words
blockchain, distributed networks

Fecha de recepción: 15-1-2018 *Fecha de aceptación: 15-5-2018*

QUÉ ES *BLOCKCHAIN*

La tecnología *blockchain* o cadena de bloques es una de las innovaciones tecnológicas que más atención ha atraído en los últimos meses. Sin embargo, dista mucho de ser una tecnología reciente, ya que sus orígenes teóricos se remontan a los años ochenta y fue al final de la década de los noventa cuando empezó a desarrollarse materialmente de forma embrionaria. Así, en 1998, Nick Szabo describió un sistema descentralizado de pagos basado en el uso de técnicas criptográficas para facilitar la generación de unidades de valor virtual de forma estructurada (sistema hoy conocido como *proof-of-work*)[1].

Posteriormente, en un artículo publicado en 2008[2], Satoshi Nakamoto, cuya misteriosa identidad sigue alimentando leyendas urbanas[3], propuso una solución técnica para realizar transacciones entre dos agentes sin la necesidad de contar con una autoridad o institución que actuase como entidad compensadora o validadora de la transacción. Como anunciaba el título de su trabajo, *Bitcoin: a Peer-to-Peer electronic cash system*, el sistema propuesto por Nakamoto se materializó en el año 2009 con el nacimiento de la red *Bitcoin*, la primera red *blockchain*.

Sin embargo, *blockchain* no es *Bitcoin*. Es mucho más. *Blockchain* es una tecnología con aplicaciones descritas, y materializadas ya, en multitud de campos más allá de las llamadas monedas virtuales[4]. Su forma de funcionamiento, ciertamente disruptiva del modelo de confianza que subyace a nuestra cultura y basa nuestro Derecho, determinará el éxito o el fracaso de su aplicación en cada campo. En

* Del Área de Derecho Público, Procesal y Arbitraje de Uría Menéndez (Barcelona).
Con nuestro agradecimiento al Dr. Josep Pegueroles, Universitat Politècnica de Catalunya (Departament d'Enginyeria Telemàtica), por su revisión técnica de nuestro texto.

1 *Irish Department of Finance*: *Discussion Paper: Virtual Currencies and Blockchain Technology*, marzo 2018, pág. 3 (http://www.finance.gov.ie/wp-content/uploads/2018/03/Virtual-Currencies-and-Blockchain-Technology-March-2018.pdf).

2 NAKAMOTO, Satoshi: *Bitcoin: a Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf

3 La identidad del creador de *bitcoin* se ha atribuido a distintas personas, desde el mismo Nick Szabo hasta un coleccionista japonés de maquetas de trenes, pasando por el australiano Craig Steven Wright, quien sigue afirmando ser la persona que se esconde tras el seudónimo. Otras fuentes afirman que Satoshi Nakamoto no es una persona, sino que se trata del acrónimo de las compañías Samsung, Toshiba, Nakamichi y Motorola (KIM, Larry: *15 Weird and Interesting Facts and Theories About Satoshi Nakamoto, the Founder of Bitcoin*, 13 de abril de 2018, en https://medium.com/marketing-and-entrepreneurship/15-weird-and-interesting-facts-and-theories-about-satoshi-nakamoto-the-founder-of-bitcoin-7fc7a6ee73c6).

4 «*The technology behind these assets—including blockchain—is an exciting advancement that could help revolutionize fields beyond finance*» (LAGARDE, Christine: «Addressing the Dark Side of the Crypto World», *IMF Blog,* 13 de marzo de 2018, en https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/).

este sentido, en nuestra opinión, es imprescindible conocer las características de su funcionamiento para que afloren las cuestiones jurídicas que sus aplicaciones suscitan en las distintas disciplinas de nuestro ordenamiento.

Así, dedicamos la primera sección de este trabajo a explicar las características básicas de esta tecnología para un no técnico; la segunda, a describir aplicaciones esbozadas o materializadas ya en la actualidad; y la tercera y última, a reflexionar brevemente sobre los retos jurídicos que tal materialización, a nuestro modo de ver, plantea.

CÓMO FUNCIONA *BLOCKCHAIN:* UNA BREVE EXPLICACIÓN TÉCNICA

Su base: la tecnología del registro distribuido

Desde antiguo, desde siempre, empresas e instituciones han utilizado libros para crear y mantener, mediante asientos y anotaciones, registros de transacciones o movimientos. Los titulares de esos libros (Administraciones públicas, bancos, empresas, etc.) concentran, así, información relevante y están en posición de consultarla. En consecuencia, pueden actuar como intermediaros cuando otros agentes interesados precisan de tal información para realizar transacciones, pero, por no ser pública o por necesitar ser validada, no pueden de otra forma conocer o utilizar[5].

Así las cosas, el titular o garante de la información se convierte en una «autoridad central», en «*un intermediario en quien todos los usuarios confían, que tiene un control total sobre el sistema e interviene en todas las transacciones*»[6]. No debemos equiparar esta «autoridad central» a una autoridad pública ni a una entidad de crédito u otro tipo de entidad regulada en particular. Se trata, simplemente, del término que se emplea en los trabajos sobre esta tecnología para identificar al poseedor de la información en el sistema tradicional basado en la confianza, el sistema «centralizado».

Pues bien, la tecnología *blockchain* se presenta como capaz de dar un giro a este sistema, puesto que, mediante un protocolo informático de código abierto[7], permite la llevanza de bases de datos de forma descentralizada, «distribuida», sin necesidad, así, de contar siempre y en todo caso con una «autoridad central», o entidad poseedora de la información, que actúe como garante de su corrección y como intermediaria en las transacciones realizadas sobre su base.

La tecnología *blockchain*, como *distributed ledger technology* o *DLT* (tecnología de red o registro distribuido) que es, permite crear redes para compartir libros registro de transacciones electrónicas, muy similares a los libros de contabilidad (*ledger*[8]); o, dicho de otro modo, bases de datos digitales compartidas. Su singularidad reside en el hecho de que estos libros están distribuidos (*distributed*) entre los participantes de la red, quienes se encargan —todos ellos— de su llevanza[9].

En este tipo de redes, cada uno de los nodos o usuarios (ordenadores) tiene una copia original

5 BOUCHER, Philip: «How blockchain technology could change our lives», *In-depth Analysis*, *European Parliamentary Research Service,* febrero 2017, pág. 5, http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf.

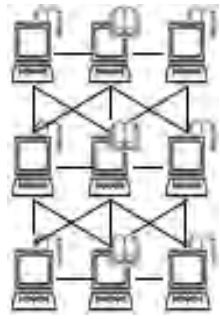
6 BOUCHER, Philip, *op. cit.*, pág. 5.

7 Existen muchas definiciones sobre qué debe entenderse por *software* de «código abierto» u «*open source*» (muchas diferenciándolo del llamado «*software* libre»). Reseñamos aquí la de un autor publicado por la Organización Mundial de la Propiedad Intelectual (OMPI), DAVIDSON, Stephen J.: *Estudio sobre los programas informáticos de código abierto*, Minneápolis, 2004, en http://www.wipo.int/sme/es/documents/opensource_software_primer.htm#alg.
Dice este autor respecto del *software* de código abierto, de «*los verdaderos programas de código abierto*», que su código fuente «*está disponible a los fines de su uso, modificación y distribución «libre», aunque la licencia correspondiente puede quedar sujeta a ciertas condiciones u obligaciones que obstaculizan su uso comercial…*».
Lo anterior debe leerse con sus descripciones previas de «código» y «código fuente». Dice textualmente «*La palabra «código» se refiere al código fuente de los programas informáticos. Los programas informáticos y sistemas operativos suelen escribirlos personas que utilizan un lenguaje de programación determinado. Es lo que se llama el código fuente del programa. Para que el computador pueda utilizar realmente un programa, lo tiene que traducir del código fuente a un idioma informático que el computador pueda entender y ejecutar.* […] *Para cambiar un programa, el programador cambia el texto del código fuente y después genera una nueva versión del programa a partir de él. En general, la modificación o reparación de un programa está limitada por el creador original del programa, algo que no se puede evitar a no ser que se disponga del código fuente pertinente*».

8 «Ledger»: «A book or other collection of financial accounts», en *Oxford English Dictionary online*, (2018), https://en.oxforddictionaries.com/definition/ledger; y «Ledger»: «a book in which things are regularly recorded, especially business activities and money received or paid», en *Cambridge English Dictionary online*, (2018), https://dictionary.cambridge.org/dictionary/english/ledger.

9 European Securities and Markets Authority (ESMA): *Report. The Distributed Ledger Technology Applied to Securities Markets*, 7 de febrero de 2017, pág. 4, https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

Red centralizada: los usuarios no tienen su propia copia del libro registro. Para realizar transacciones entre ellos deben recurrir a una autoridad central validadora, que sí tiene la información.



Red distribuida: cada usuario tiene su propia copia del libro registro. Los usuarios pueden realizar transacciones entre sí.

del libro registro y, por lo tanto, cada uno de ellos es capaz de determinar si las operaciones planteadas por el resto de los usuarios de la red pueden realizarse o no. La llevanza de libros registro distribuidos la realizan, en consecuencia, los propios usuarios de la red *blockchain* sobre la que se ha desarrollado la concreta base de datos en cuestión. Este hecho significa que todas las transacciones que se realizan en tal red son aprobadas y validadas por los propios nodos, que son capaces de verificarlas y validarlas mediante cotejo con su propia copia del libro registro. Tal aprobación se lleva a cabo por consenso, de modo que cuando la mayoría de los nodos está de acuerdo con una actualización del libro registro (*i.e.*, la incorporación de nuevas transacciones), el contenido aprobado queda incorporado por la propia decisión del grupo, sin necesidad de intervención de entidad validadora o certificadora de la información. Una vez que los nodos consensúan la inclusión de una nueva transacción en el libro registro, este se actualiza y la nueva versión deviene firme.

CÓMO SE INCORPORA LA INFORMACIÓN AL LIBRO REGISTRO DISTRIBUIDO: LA CADENA DE BLOQUES

En el libro registro, todas y cada una de las transacciones se agrupan en bloques, que no son más que «paquetes» con la información sobre las últimas transacciones realizadas en un determinado periodo de tiempo. Estos bloques se van añadiendo de forma sucesiva al libro registro en la red a medida que se van formando. Cuando un bloque de información se incorpora al libro registro, queda irreversiblemente vinculado al bloque aprobado anteriormente, de modo que se encadenan entre ellos, y de ahí que esta tecnología se denomine «cadena de bloques». Esta vinculación entre los bloques es posible gracias a un robusto sistema criptográfico, que convierte las redes *blockchain* en registros prácticamente inalterables.

El ejercicio de validar las transacciones, la creación de los bloques y su posterior incorporación al registro distribuido es realizado por los llamados nodos validadores. Estos usuarios de la red cotejan su versión del libro registro con las transacciones constantemente propuestas por los usuarios para verificar que (i) el usuario emisor y el receptor tienen cuentas que existen y (ii) el emisor tiene disponible aquello que quiere transferir o mover. Si el contenido de la transacción es coherente con la copia del libro registro distribuido del nodo validador, este la incluirá en un bloque. Una vez que el bloque se «llena» de transacciones propuestas[10], el nodo validador lo someterá a la aprobación del resto de los nodos validadores, que lo aprobarán si, nuevamente, el contenido coincide con su respectiva versión del registro.

Si la mayoría de los usuarios no acepta el contenido, esta parte del bloque no será incorporada al registro. Ahora bien, una vez que un bloque se añade al registro, no puede eliminarse de ningún modo: mientras que destruir o corromper un

10 Los bloques poseen un límite máximo de capacidad de información.

registro tradicional requiere un ataque al intermediario, un sistema *blockchain* requiere un ataque simultáneo a un porcentaje significativo de copias del libro registro, que, por encontrarse físicamente almacenadas en el ordenador de cada usuario, son de muy compleja alteración en la mayoría de redes[11].

UN EJEMPLO PRÁCTICO: UNA TRANSACCIÓN SENCILLA CON *BITCOINS*

Imaginemos ahora que A, un usuario de una red *blockchain*, desea realizar una transferencia de dos bitcoins (BTC) a otro usuario de la red, B. Para poder realizar la transferencia, A y B deben descargar previamente el *software* correspondiente para acceder a la concreta red *blockchain* (Bitcoin, en nuestro ejemplo); obtener las claves criptográficas que servirán para «firmar» y desencriptar los mensajes enviados a la red; y crear una cuenta en un monedero virtual (*wallet*) a través de Internet. Una vez que cumplan con estos requisitos, los pasos a seguir serán los siguientes:

1. A propondrá una transacción al resto de los nodos, consistente en que dos BTC registrados en su cuenta pasen a estar registrados en la cuenta de B y se eliminen de la suya. El mensaje de A incluirá (i) la cantidad de BTC a transferir (aquí, 2) y (ii) la dirección a la que se transferirán (cuenta de B).
2. El mensaje con la transacción propuesta será recibido de forma encriptada por los nodos validadores, que verificarán (i) que la proposición de transacción ha sido enviada por el usuario que debe transferir los BTC (en nuestro caso, por A), (ii) que el usuario dispone de la cantidad de BTC que desea transmitir y (iii) que el usuario destinatario existe.
3. Si el mensaje de A es correcto, los nodos validadores calcularán su *hash*[12]. El *hash*, equiparable a una huella dactilar o elemento específico de cada transacción, permite identificar una transacción de forma individualizada, puesto que se obtiene a partir de su concreto contenido y es único[13].
4. La transacción verificada se incluirá en un bloque, es decir, en un paquete de información que contiene las últimas transacciones recibidas y verificadas en un determinado lapso de tiempo. Cada bloque incluye:
   a. el *hash* del bloque anterior;
   b. el *hash* raíz: el *hash* resultante de aplicar el algoritmo al conjunto de los *hash* de todas las transacciones que integran el bloque;
   c. el sello temporal del bloque (*i.e.*, día y hora en que el bloque se ha aprobado); y
   d. el *hash* del propio bloque: aplicar la función *hash* al conjunto de (a, b y c).
5. Antes de poder «cerrar el bloque» e incluirlo en la cadena, el nodo validador realiza cálculos para resolver un problema matemático consistente en hallar una combinación numérica (el llamado *nonce*), que debe colocarse al inicio del *hash* y que solamente puede ser resuelto mediante prueba y repetición[14].
6. La nueva versión del libro registro es remitida a todos los nodos.

CARACTERÍSTICAS DEL *BLOCKCHAIN* Y TIPOS DE REDES

A la vista de lo anteriormente expuesto, creemos que tres de las características de la tecnología *blockchain* son especialmente relevantes en el planteamiento de las cuestiones jurídicas que suscitan las

11 BOUCHER, Philip, *op. cit.*, pág. 5.

12 El *hash* es una concatenación de caracteres alfanuméricos que resultan de aplicar un algoritmo matemático sobre un archivo u objeto digital cualquiera. En el caso de la red Bitcoin, el algoritmo usado para calcular el *hash* es el SHA-256, que produce una combinación de 64 caracteres. El *hash* resultante de aplicarlo a cada archivo es inmutable; será el mismo cada vez que se calcule. Ahora bien, el *hash* variará si se altera el contenido de este, por mínima que sea la variación. Por ello decimos que el *hash* es único para cada archivo u objeto al que se aplica. Asimismo, el *hash* no es reversible, sino que es unidireccional. Puede calcularse el *hash* de un archivo, pero no puede obtenerse el archivo original a partir del *hash*.

13 Agencia Española de Protección de Datos: *Orientaciones y garantías en los procedimientos de Anonimización de datos personales*, 2016, págs. 17 y ss., https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf); y GONZÁLEZ-MENESES, Manuel: *Entender Blockchain. Una Introducción a la Tecnología de Registro Distribuido*, Cizur Menor, 2017, págs. 74 y ss.

14 Este último paso previo a «cerrar los bloques» no es común en todas las redes *blockchain*, tal y como veremos en el siguiente apartado. Esta actividad recibe el nombre de «minería».

aplicaciones de esta tecnología. Estas características son las siguientes:

(i) Transparencia

Partiendo de la base de que todos los usuarios de las redes *blockchain* tienen acceso al libro registro, ello implica que todos tienen la información sobre las transacciones que se efectúan por el grupo. Es más, en determinadas redes —no en todas—, los usuarios que no forman parte de la red también pueden consultar el contenido de la cadena de bloques. Así ocurre, por ejemplo, en las redes Bitcoin o Ethereum. A esto se añade, además, que se trata de protocolos informáticos de código abierto, por lo que el acceso al diseño de la programación es también libre.

Esta transparencia, sin embargo, no significa que podamos conocer al autor de las transacciones en todo caso. En algunos tipos de redes los usuarios no necesitan identificarse de forma personal para acceder y operar en la correspondiente red *blockchain*. Las transacciones son visibles, pero vinculadas a un código. Esta característica ha ocasionado que se hayan vinculado algunas de estas redes a actividades ilícitas por el carácter anónimo en la actuación que permiten en ciertos casos.

(ii) Irrevocabilidad

Una vez que la información se incorpora a una red *blockchain*, en general (salvo ciertas excepciones), no es posible eliminarla de allí. En otras palabras, no hay marcha atrás. La información es poseída por todos los usuarios, por lo que es imposible eliminarla de la red. Los datos incorporados a la cadena de bloques se distribuyen a todos y cada uno de los nodos que intervienen en ella.

(iii) Inmutabilidad

Como consecuencia del encadenamiento sucesivo de los bloques basado en la criptografía (los *hash*), el contenido de la cadena de bloques es inmutable. Si un nodo decide cambiar el contenido de la cadena de bloques alterando una transacción ya realizada e incluida en un bloque, provocará que el contenido de su versión del libro registro varíe, un cambio que será fácilmente identificable por el resto de los nodos. Por lo tanto, a la hora de someter a aprobación una nueva transacción, estos no aceptarán su versión del registro, puesto que el contenido será distinto.

Estas tres propiedades son atribuibles de forma general a las redes *blockchain*. Sin embargo, existen otros parámetros que los desarrolladores tienen en cuenta y deciden a la hora de configurar estas redes, dependiendo de la función a la que cada red esté destinada, y que permiten matizar lo que acabamos de exponer. En particular, en función de las decisiones sobre algunos de estos parámetros, las redes *blockchain* pueden ser públicas o privadas:

- Redes **públicas**: no exigen a los usuarios el cumplimiento de ningún requisito para poder unirse a ellas *(e.g.*, requisitos de identificación) y no existe ninguna jerarquía entre los nodos, por lo que cualquier nodo puede convertirse en nodo validador si lo desea. El contenido de la cadena de bloques es transparente y visible para todos los usuarios (en algunos casos, incluso para aquellos que no son usuarios de la red). Puesto que estas redes no exigen permiso o invitación alguna para poder acceder y participar, reciben el calificativo de *permissionless*.

Para evitar el fraude, los nodos validadores, además de realizar las operaciones de validación, deben resolver un conjunto de problemas criptográficos antes de poder incorporar un nuevo bloque a la cadena de bloques (este tipo de sistema recibe el nombre de *proof-of-work*, como el ideado en su día por Nick Szabo). Puesto que para realizar estas tareas los nodos validadores deben poner a disposición de la red su poder computacional, con los gastos energéticos y a nivel de infraestructura que ello comporta[15], reciben una compensación por realizar esta tarea. En gran parte de las redes públicas, este incentivo se traduce en la recepción de una pequeña comisión al primer nodo validador que consigue resolver el problema criptográfico. Estos nodos validadores son también conocidos como «mineros» y su acción como «minar» o «minería».

- Redes **privadas**: un grupo limitado de actores conserva el poder de acceder, comprobar y añadir transacciones al libro registro[16]. Este grupo también está en posición de decidir qué nuevos usuarios

15 Aunque en los inicios de las redes *blockchain* el minado podía realizarse mediante un ordenador corriente, la especialización y la profesionalización de los mineros es cada vez mayor (POPPER, Nathaniel: «There Is Nothing Virutal About Bitcoin's Energy Appetite», *The New York Times*, 21 de enero de 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html?ref=nyt-es&mcid=nyt-es&subid=article). La enorme exigencia energética de esta tecnología ha sido mencionada en muchas ocasiones como un factor determinante de su inviabilidad (BBC Mundo. Redacción: *Por qué se gasta tanta electricidad para producir bitcoins (y qué tan cierto es que consume tanta energía como Dinamarca)*, 12 de diciembre de 2017, http://www.bbc.com/mundo/noticias-42323617).

16 BOUCHER, Philip, *op. cit.*, pág. 5.

podrán incorporarse a la red y bajo qué requisitos (por ejemplo, tener relación laboral o de clientela con una determinada empresa, ser propietario de una determinada comunidad, pertenecer a un concreto grupo empresarial, etc.). Así, además, estas redes exigen el cumplimiento de determinados requisitos a aquellos usuarios que desean incorporarse a la red (*e.g.*, identificación, procedimientos de KYC, etc.). Asimismo, también puede existir jerarquía entre los nodos, de modo que no cualquier usuario puede convertirse en un nodo validador o tener acceso a todos los datos sobre los usuarios. En este tipo de redes, los nodos validadores son nodos «de confianza» (en la acepción tradicional del término), esto es, entes en quienes todos los usuarios confían y que no necesitan ningún incentivo para realizar las tareas de validación (de modo que los «mineros» no son necesarios). En la terminología específica, el antes mencionado sistema *proof-of-work* se sustituye en estos casos por un sistema *proof-of-stake* o *proof-of-authority.* El proceso de validación de transacciones es más rápido que el de las redes públicas, a la vez que consume menos energía[17]. También se suele mantener que el encargo de la gestión solamente a participantes leales y la reducción de los procesos requeridos para su funcionamiento reducen igualmente el riesgo de sufrir ciberataques y brechas de seguridad[18]. Por todo ello, estas redes reciben el calificativo de *permissioned*.

Las redes privadas pueden tener distintos niveles o grados de apertura, desde redes para grupos cerrados en las que los anteriores requisitos se cumplen en su grado máximo hasta redes que prácticamente se podrían cualificar de públicas, en su modo de funcionamiento, pero que, eso sí, tienen requisitos de acceso y utilización a modo de términos y condiciones de servicio, por lo que, en rigor, no son públicas ni privadas puras. Entre las unas y las otras existe un abanico de combinaciones, que, en su configuración y régimen contractual de funcionamiento, pueden dar respuesta a muchas de las cuestiones jurídicas que plantea el modo de funcionamiento de esta tecnología.

APLICACIONES DE LA TECNOLOGÍA *BLOCKCHAIN*

Con carácter general, habida cuenta de sus características, tal y como han quedado expuestas en el apartado anterior, la utilización de esta tecnología podría aportar valor añadido, teóricamente, a aquellas actividades que cumplan con las siguientes condiciones: (i) requieran almacenar datos, (ii) precisen que el acceso a estos datos sea compartido entre diferentes partes y (iii) estas partes no se conozcan entre ellas o no exista confianza mutua por otro motivo.

Son muchas las actividades que se desarrollan o pueden desarrollarse bajo los anteriores parámetros, por lo que la utilización del *blockchain* se ha descrito, y se está desarrollando ya materialmente, en multitud de sectores y para un sinfín de aplicaciones. A continuación presentamos algunas.

CRIPTOMONEDAS

El Banco Central Europeo definió ya en 2012 las «criptomonedas» o «monedas virtuales» como «*un tipo de dinero digital y no regulado, normalmente emitido y controlado por sus desarrolladores, y usado y aceptado entre los miembros de una concreta comunidad virtual*»[19]. Con posterioridad, en la recientemente aprobada Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo[20], se definen las «monedas virtuales» como una «*representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*»[21].

Como se observa, tanto la definición del Banco Central Europeo como la de la Quinta Directiva de

17 ASTRI: «Whitepaper On Distributed Ledger Technology», *Hong Kong Monetary Authority,* 11 de noviembre de 2016, pág. 34, http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf.

18 ASTRI, *op. cit.*, pág. 11.

19 European Central Bank: *Virtual Currency Schemes*, octubre 2012, pág. 5, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

20 Aprobada el pasado 26 de abril de 2018 y pendiente de publicación en el DOUE al cierre de este trabajo: http://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf.

21 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0178+0+DOC+XML+V0//ES#BKMD-5.

Blanqueo son tecnológicamente neutras, puesto que no incluyen la utilización de la cadena de bloques, u otra tecnología, como presupuesto de la definición. Lo cierto es, no obstante, que las denominadas criptomonedas se vienen creando, distribuyendo e intercambiando sobre tecnología *blockchain*. Son, en definitiva, apuntes contables en un libro registro digital y compartido entre los usuarios de una comunidad, quienes le atribuyen un valor.

Hoy en día existen miles de criptomonedas, cientos de ellas son creadas cada semana, aunque las más extendidas son el *bitcoin* (BTC) y el *ether* (ETH). Las redes Bitcoin y Ethereum tienen elementos comunes, pero se diferencian en algunos aspectos:

— **Bitcoin**: Red creada en 2009. Está programada para finalizar la emisión de bitcoins cuando se alcance la cifra de 21 millones de BTC emitidos. La red Bitcoin está diseñada para funcionar como medio de pago entre aquellos que deciden voluntariamente aceptarlo como tal.

— **Ethereum**: Red creada en 2015 por Vitalik Buterin. Aunque la emisión de *ethers* es, en principio, ilimitada, la emisión anual está limitada a 18 millones de unidades[22]. La principal diferencia con la red Bitcoin es que la red Ethereum permite realizar transacciones más sofisticadas que el mero pago, al admitir que operen sobre su estructura ciertos *smart contracts*, a los que nos referiremos más adelante.

ICO (*INITIAL COIN OFFERINGS*) E ILP (*INITIAL LOAN PROCUREMENTS*)

Aunque originariamente fueron creados para funcionar como medio de pago, los activos virtuales rápidamente se convirtieron en valor de cambio de distintas contraprestaciones, incluyendo nuevos modos de captación de fondos de inversores para financiar futuros negocios. En este ámbito, los promotores de las llamadas ICO (*Initial Coin Offering*) ofrecen, a cambio de moneda de curso legal o moneda virtual, un *token*, una especie de vale virtual, instrumentado como apunte digital del derecho a la obtención de distintos beneficios posibles, como el acceso o posibilidad de adquisición de un producto o servicio todavía no lanzado al mercado (*utility tokens*), o, incluso, un interés participativo en los futuros ingresos o el posible aumento del valor de la entidad emisora o del negocio (*equity tokens*)[23]. Proyectos de muy distinta índole tienen su origen en una ICO. En el 2017 fueron lanzadas 210 ICO, y solo en los primeros cuatro meses de 2018, 212[24].

Al igual que las ICO, los recién surgidos ILP (*Initial Loan Procurements*) se están destinando a captar fondos para nuevos proyectos. En este caso, los usuarios que deciden acudir a la oferta reciben *tokens* de acceso a derechos de crédito transmisibles a terceros o FLATS (*Future Loan Access Tokens*). La aportación se articula a través de un contrato de préstamo con el receptor de los fondos en formato *smart contract*, código autoejecutable, en cuya virtud el prestador recibe los pagos de forma automática y sin la intervención de operador alguno[25].

Sus valedores defienden que los ILP permiten que los beneficios de los inversores no estén condicionados por la volatilidad de sus *tokens*, como sucedería a su decir en el caso de las ICO, puesto que el retorno solamente depende de los beneficios que el negocio llegue a obtener cada año (lo que, de hecho, supuestamente también sucede bajo algunas formas de ICO). Aunque mucho menos numerosos que los de ICO, los ejemplos de ILP son una realidad en algunos países (especialmente en Estonia).

SMART CONTRACTS

Los denominados *smart contracts* o «contratos inteligentes», que hemos mencionado ya al referirnos a las posibilidades técnicas de la red Ethereum y a la devolución automática al prestador en los ILP, se suelen describir como «contratos» autoejecutables. Si son o no contratos dependerá en cada caso de si concurren los requisitos de consentimiento, objeto y causa para ello. En cualquier caso, en rigor, la aptitud para ser jurídicamente contrato no corresponde a lo que comúnmente se conoce como *smart contract*, y que no es más que programa autoejecu-

22 Irish Department of Finance, *op. cit.*, pág. 2.

23 Comisión Nacional del Mercado de Valores: *Comunicado difundido por la Securities and Exchange Commission con consideraciones de su presidente sobre las criptomonedas y las denominadas «ofertas iniciales de criptomonedas» («Initial Coin Offerings» o «ICOs»)*, enero de 2018, págs. 6 y 7, http://www.cnmv.es/portal/verDoc.axd?t=(14a617e8-7f18-40e0-9f1b-2061d924f5f4).

24 https://www.coinschedule.com/stats.html?year=2018.

25 SAYER, Luke: «Goodbye ICOs, hello ILPs?», *Business Brief*, 346, 2018, págs. 34-35.

table, sino a lo que se ha denominado «contrato legal inteligente», del que el *smart contract* es solo parte, y que se ha definido como el contrato celebrado «*a través de una página web accesible para las partes cuya forma está constituida por la interfaz de usuario de la aplicación externa y uno o varios programas autoejecutables (smart contracts) residentes en la cadena de bloques con capacidad para actuar recíprocamente con dicha interfaz*» [26].

Así, los *smart contratcs* son, como avanzábamos, programa autoejecutable, o, mejor, el uso de código informático para conseguir que la ejecución de acuerdos de voluntad sencillos no dependa de la contraparte ni de terceros[27]. Son, en otras palabras, la «traducción» a código informático de reglas o acuerdos alcanzados a dos o más partes para su autoejecución. Algo que, en realidad, no es nuevo, pero a lo que el *blockchain* ha abierto enormes oportunidades. El código contiene instrucciones, almacenadas en una red *blockchain*, para que, en el acontecimiento de unas determinadas circunstancias, tengan lugar unas concretas consecuencias («si X, entonces Y»)[28].

Las aplicaciones de los *smart contracts* se han apuntado en múltiples sectores. En el sector de los seguros, por ejemplo, se ha descrito su utilización para el pago automático de indemnizaciones una vez constatado el acaecimiento de ciertos tipos de siniestros. También se defiende que los *smart contracts* vinculados al *Internet of Things* (IoT) pueden permitir que los objetos, utensilios y máquinas contraten o realicen actuaciones por sus dueños, como por ejemplo un coche capaz de contactar con el taller para programar su revisión técnica cuando por kilometraje llegue el momento.

REGISTRO DE TRAZABILIDAD

La inmutabilidad del registro que los usuarios van formando sucesivamente —una de las principales características de la tecnología *blockchain*— permite crear bases de datos de información que son calificadas por sus defensores como prácticamente inalterables. Esta propiedad está siendo aprovechada y desarrollada de forma amplia por multitud de iniciativas, de muy diversa índole, que tienen como objetivo común el establecimiento de registros de información con prueba de movimientos y trazabilidad.

El común denominador de estos registros es la creación de una «identidad digital» de cada elemento que se registra, que tiene a partir de ese momento un historial propio y trazable. Toda vez que la cantidad y el tipo de información «pública» en cada registro puede ser mayor o menor en función del concreto diseño de la red *blockchain* y los permisos que se otorguen al efecto a cada usuario, las aplicaciones como herramienta de trazabilidad son muy diversas.

En el ámbito de los bienes materiales, estos registros se presentan como especialmente útiles para la identificación y el seguimiento del origen de los bienes y de su cadena de custodia. Mediante la creación de una «identidad digital» es posible identificar los productos en origen y añadir a la red información que los concierne. Así, existen desarrollos conjuntos de sistemas de trazabilidad específicos en redes *blockchain* según las necesidades de un particular sector, como por ejemplo sistemas de trazabilidad de alimentos[29] o de bienes de gran valor[30].

La trazabilidad en red *blockchain* también ha alcanzado el campo de los bienes inmateriales. Se ha descrito en particular la utilidad de un registro de estas características para la trazabilidad de la explotación de las obras en soporte digital. Una vez creada la «identidad digital» de la obra, sería posible acreditar su autenticidad, identificar al autor, registrar sus sucesivas transmisiones, sus actos de explotación, conocer el alcance y asegurar la validez de las licencias obtenidas, etc. Existen iniciativas que defienden que estos registros, vinculados al uso de

26 TUR FAÚNDEZ, Carlos: *Smart contracts, análisis jurídico*, Editorial Reus, Madrid, 2018, pág. 60.

27 STOKES, Miguel y FREIRE, Gabriel: «Smart contracts», *Actualidad Jurídica Uría Menéndez*, 46, 2017, pág. 124: «*código de programação de computador que permite, por operação do propio computador, monitorizar e/ou executar um contrato, sem necessidade de interferencia humana*».

28 Un análisis exhaustivo del lenguaje y la forma de los *smart contracts* y de las cuestiones jurídicas que plantean es el realizado por Jorge Feliu en: FELIU REY, Jorge: «Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado», *La Ley Mercantil,* n.º 47, 2018.

29 Según información de IBM en https://www.ibm.com/blockchain/supply-chain/, Walmart e IBM están desarrollando un sistema de trazabilidad de alimentos en cadena de bloques que permitirá a los consumidores obtener muy diversa información sobre los productos que adquieran en el supermercado, como su origen, modo de producción, días hasta la caducidad, etc.

30 El Proyecto Everledger, desarrollado por su promotores también en colaboración con IBM (www.everledger.io), busca proporcionar en *blockchain* el historial de las sucesivas transmisiones de propiedad y garantizar la licitud del origen y autenticidad de piedras preciosas.

monedas virtuales y *smart contracts*, permiten la gestión directa de forma muy sencilla de los derechos económicos o de explotación de las obras objeto de derechos de autor, haciendo rentable cualquier acto de explotación, por pequeño que este sea, al permitir el pago automático de *royalties* a los autores, aunque se trate de importes muy reducidos, toda vez que las criptomonedas permiten, como explicamos a continuación, su división en unidades de valor muy pequeñas.

HERRAMIENTA PARA MICROPAGOS

Los activos virtuales permiten técnicamente, en efecto, su división y subdivisión en unidades ínfimas. Si a ello le sumamos el carácter colaborativo al que frecuentemente se ha vinculado esta tecnología, multitud de iniciativas defienden que, con su uso, los micropagos son posibles, y rentables, y que, por lo tanto, también son posibles nuevas formas de gestión y explotación de muchos activos.

Así, por ejemplo, antes ya nos hemos referido a plataformas en cadena de bloques que permiten a los autores adheridos cobrar, directamente de los usuarios y casi a tiempo real, por el uso y explotación de sus obras objeto de propiedad intelectual. En el sector de la energía, la tecnología que nos ocupa se ha empleado ya para la realización de micropagos en la compraventa de energías renovables entre miembros de comunidades locales productoras. En el sector de la publicidad, existen proyectos para la instrumentalización más rápida y eficiente del cobro y pago de los precios vinculados al número de visualizaciones del contenido anunciado.

GOBERNANZA DE ORGANIZACIONES

La tecnología *blockchain* también se ha presentado como una buena herramienta para agilizar la gestión y gobernanza de las organizaciones, por dotar a las votaciones electrónicas de mayor seguridad y transparencia en el proceso, permitiendo, a su vez y cuando sea preciso, el anonimato en las consultas. La combinación de estas propiedades con sus utilidades en materia de gestión documental y los parámetros de la firma electrónica han conducido a que esta tecnología se presente como muy útil para la creación de un registro inalterable de la vida corporativa.

La expresión más extrema de organizaciones gobernadas de forma descentralizada son las denominadas DAO (*Descentralized Autonomous Organizations*), entidades regidas por decisiones tomadas automáticamente mediante conjuntos de *smart contracts*. Más allá del debate a nivel jurídico, son entes cuestionados desde muchas otras perspectivas[31].

SECTOR PÚBLICO

No son pocas las iniciativas que valoran las utilidades de la tecnología *blockchain* para mejorar la eficiencia en procesos guiados por el interés público. Dentro de la Unión Europea, Estonia busca liderar el proceso de transformación digital y, en este marco, trabaja para que la cadena de bloques ayude a los ciudadanos a realizar el mayor número de gestiones posibles mediante su identidad digital[32]. En Reino Unido, el Bank of England ha anunciado su intención de reformar su actual sistema de compensación RTGS (*Real-time gross settlement*) para hacerlo compatible con la tecnología DLT[33]. Suecia, por su lado, trabaja la forma de realizar transacciones inmobiliarias íntegramente a través de *blockchain*[34].

Fuera de Europa, países como Ghana, Kenia y Nigeria han empezado a utilizar redes *blockchain* para gestionar sus registros de la propiedad[35] y, así, mejorar problemas como la corrupción, la existencia de áreas indocumentadas, las dificultades para conservar la integridad de los registros físicos o el bajo nivel de acceso a los registros públicos. Y diversos estados (entre ellos, Canadá y Japón) han planteado una posible emisión de monedas virtuales de curso legal («*Central Bank Digital Currency*», o «BDC»). En el caso de Japón, está previsto que su «moneda virtual», el J-Coin, sea lanzada a tiempo para los Juegos Olímpicos de Tokio en 2020[36].

---

31 En particular, por razón de su vulnerabilidad ante ciberataques, como quedó de manifiesto cuando, en 2016, según las noticias de prensa publicadas, la organización autónoma descentralizada «The DAO» fue atacada debido a un error de código y 3,6 millones de ethers pertenecientes a terceros fueron sustraídos y trasladados a otra DAO.

32 e-Estonia permite acceder a multitud de servicios digitales: https://e-estonia.com/.

33 Bank of England: *RTGS Renewal Proof of Concept: Supporting DLT Settlement Models*, 27 de marzo de 2018, https://www.bankofengland.co.uk/news/2018/march/rtgs-renewal-proof-of-concept.

34 BOUCHER, Philip, *op. cit.*, pág. 18.

35 http://www.bitland.world/about/.

36 WILLIAMS-GRUT, Oscar: «Japan wants to launch a new digital currency: J-Coin», *Business Insider UK*, 26 de septiembre de

RETOS JURÍDICOS RELACIONADOS

Como se comprenderá, ante la diversidad de aplicaciones de esta tecnología, se han alzado voces reclamando su inmediata regulación. Así ha sucedido muy especialmente en relación con su utilización como plataforma de transacción de activos virtuales con asignación de valores de intercambio (monedas virtuales, ICO, ILT, etc.)[37].

Las autoridades comunitarias han adoptado hasta ahora una posición de cautela frente a estas iniciativas, por lo que el común denominador en sus comunicaciones han sido los mensajes de alerta frente a los potenciales riesgos para usuarios e inversores (*grosso modo*, el riesgo de perder la inversión dada la alta volatilidad de los activos y la falta de protección y garantías). Aun así, la Unión Europea y sus autoridades han manifestado que con ello no pretenden obstaculizar la innovación tecnológica, ni en particular el *blockchain*, y prueba de ello son las menciones a esta circunstancia en los comunicados emitidos por diversas autoridades y la propia creación del EU Blockchain Observatory & Forum[38]. En España, las autoridades también se han mostrado proactivas en cuanto al fomento de la innovación en el ámbito de la tecnología blockchain. Un ejemplo de ello es la prueba piloto para la simplificación de procesos y reducción de tiempos en el registro de emisiones utilizando tecnología blockchain que vienen realizando durante el último año la CNMV y Bolsas y Mercados Españoles de forma conjunta con diversas entidades.

En cualquier caso, como decíamos, los comunicados, opiniones y estudios publicados por las instituciones son de cautela y giran en torno a los siguientes motivos de alerta: (i) la falta de regulación de estas actividades y su posible vinculación a actividades ilegales o fraudulentas; (ii) el alto riesgo de pérdida del capital invertido, dado el estado embrionario de muchos de los negocios vinculados a las ICO; (iii) la falta de liquidez de la inversión y una alta volatilidad; (iv) la información deficiente a los inversores sobre los proyectos; y (v) los posibles fallos en la tecnología.

La Autoridad Bancaria Europea (EBA) fue la primera en advertir a los consumidores, en diciembre de 2013, sobre los riesgos derivados de comprar, poseer y operar con criptomonedas[39]. Posteriormente, en 2014, realizó otro análisis de riesgos y recomendaba la instauración de un cuerpo de regulación específica[40]. Siendo consciente de la dificultad que ello entrañaría, ya predicaba la inclusión de las casas de cambio de criptomonedas como sujetos obligados por la Directiva de Blanqueo, hecho que corroboró en 2016, extendiéndolo también a los proveedores de *wallets*[41].

La Autoridad Europea de Valores y Mercados (ESMA), por su lado, ha emitido alertas dirigidas tanto a inversores[42] como a empresas[43] sobre los riesgos inherentes a las ICO y ha recordado a las empresas cuyo negocio está vinculado a las ICO que no dejan de estar sujetas al ordenamiento vigente.

El Banco Central Europeo (BCE) se ha mostrado cauteloso acerca de la evolución de las «monedas virtuales» y, en cualquier caso, contrario a la adopción de «monedas virtuales» de curso legal en coexistencia con el euro.

2017, http://uk.businessinsider.com/japan-plans-new-digital-currency-j-coin-2017-9.

37 En realidad, incluso los propios promotores de estas actividades solicitan en algunos casos su regulación, o, al menos, el establecimiento de *regulatory sandboxes*, o espacios que les permitan iniciar sus actividades en puerto seguro. En el caso de España, las peticiones de incorporar bancos de prueba regulatorios o regulatory sandboxes han sido recogidas por las autoridades, que se han mostrado en principio receptivas al respecto. En una comparecencia ante la Comisión de Economía del Congreso de los Diputados el pasado 4 de abril, el ministro de Economía, Industria y Competitividad anunció la intención de regular la implantación de bancos de prueba regulatorios en España con el objetivo de fomentar la innovación tecnológica en el ámbito financiero y el desarrollo de empresas «fintech», objeto probable de la próxima regulación de la transformación digital del sistema financiero.

38 https://www.eublockchainforum.eu/.

39 European Banking Authority: *Warning to consumers on virtual currencies*, 13 de diciembre de 2013, https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

40 European Banking Authority: *EBA opinion on «virtual currencies»*, 4 de julio de 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

41 European Banking Authority: *Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*, 11 de agosto de 2016, https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD.

42 European Securities and Markets Authority (ESMA): *Statement. ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)*, 13 de noviembre de 2017, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf.

43 European Securities and Markets Authority (ESMA): *Statement. ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements*, 13 de noviembre de 2017, https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

Las autoridades españolas, por su parte, también han alertado a los inversores sobre los riesgos de estas prácticas. El Banco de España y la Comisión Nacional del Mercado de Valores (CNMV), en un comunicado conjunto publicado el pasado mes de febrero[44], destacaron entre sus riesgos el hecho de tratarse, precisamente, de un espacio no regulado, y no beneficiarse, por consiguiente, de las garantías o protecciones previstas en la normativa relativa a los productos bancarios o de inversión, sin perjuicio, además, de los problemas derivados del carácter transfronterizo del fenómeno, el elevado riesgo de pérdida del capital invertido, los problemas de liquidez y volatilidad extrema, así como, siempre según el Banco de España y la CNMV, el suministro de información inadecuada. En su comunicado referencian las alertas ya realizadas por la ESMA[45] e IOSCO[46], y abogan también por su regulación, ya que, por la dimensión internacional del fenómeno, es necesario que se aborde la cuestión a nivel internacional y a partir de posicionamientos conjuntos de los reguladores y supervisores del mayor número de jurisdicciones.

Ahora mismo, no obstante, más allá de numerosas alertas como las referidas, solo las plataformas de negociación con criptomonedas y los proveedores de *wallets* han sido objeto de regulación en el ordenamiento comunitario, y única y exclusivamente, además, a los efectos de incluirlos como sujetos obligados por la normativa de blanqueo de capitales en la nueva Directiva de Blanqueo, en particular en lo relativo a las obligaciones sobre procedimientos KYC, obligación de registro y de identificación de titular real.

En cualquier caso, la utilización como valores negociables o instrumentos financieros de los activos virtuales y su necesaria o innecesaria regulación son cuestiones que escapan del objeto de este trabajo, cuyo fin se limita a intentar acercar los elementos básicos de la tecnología *blockchain* al lector jurídico, con el ánimo de que los tenga en mente en el día a día de su trabajo, en el marco de su particular disciplina jurídica. Más allá y sin perjuicio de la regulación de aspectos puntuales de su utilización en aplicaciones concretas, para nosotras parece evidente que de lo que se trata es de aplicar nuestro Derecho a nuevas funciones, y, por ende, tanto a nuevos riesgos como a nuevas oportunidades.

En este sentido, y sin entrar aquí a valorar el fondo, interesa destacar la reflexión de la CNMV en uno de los dos documentos más relevantes que ha difundido desde el inicio del fenómeno que estamos tratando. Así, el mismo día en el que el Banco de España y la CNMV publicaron su ya mencionado comunicado conjunto[47], la CNMV publicaba un segundo comunicado, dirigido en esta ocasión a profesionales del sector financiero[48], en el que dejaba claro que, a su criterio, por más que una regulación específica sea deseable, el ordenamiento jurídico vigente no deja de seguir siendo aplicable a la nueva realidad del mercado[49].

Sin esperar, por lo tanto, a nuevas regulaciones, debemos aplicar nuestro ordenamiento a las materializaciones de esta tecnología. Así sucede, en realidad, respecto de cualquier otra tecnología de las muchas que día a día vienen a desarrollar, por suerte, el estado de la técnica. Es aquí, quizás, donde está el verdadero reto jurídico al que debemos enfrentarnos, y no tanto, o no solo, por la complejidad de los elementos tecnológicos, sino por la velocidad con la que se están sucediendo las innovaciones.

La complejidad tecnológica —ajena a nuestra formación como abogados— nos ha obligado ya desde siempre a atender a las explicaciones de los técnicos, con particular intensidad, entre otros campos, en el mundo del Derecho de patentes y de la operativa de

44 Banco de España (BE) y Comisión Nacional del Mercado de Valores (CNMV): *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICOs)*, 8 de febrero de 2018, https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/18/presbe2018_07.pdf.

45 ESMA *Report, op. cit.*

46 International Organization of Securities Commission (OICV-IOSCO): *IOSCO Board Communication on Concerns Related to Initial Coin Offerings* (ICOs), 18 de enero de 2018.

47 BE y CNMV, *op. cit.*

48 CNMV: *Consideraciones de la CNMV sobre «criptomonedas» e «ICOs» dirigidas a los profesionales del sector financiero*, 8 de febrero de 2018, https://www.cnmv.es/loultimo/comunicadoCNMV_ICO_ES%20final.pdf.

49 Entre otros pasajes relevantes, reza el comunicado textualmente: «*La CNMV, como el resto de supervisores europeos e internacionales, es consciente de la dificultad que puede entrañar el encaje de los instrumentos que se emiten en estas operaciones en las normas vigentes, así como de la posible falta de adecuación del marco regulatorio a algunos nuevos modelos de negocio y colaboración digital. La dificultad de aplicación de las normas en un contexto digital y esencialmente transnacional obliga además a un esfuerzo de coordinación internacional. En todo caso, la CNMV es sensible a los beneficios que pueden aportar el desarrollo tecnológico y la innovación a los servicios financieros y tendrá especialmente en cuenta al ejercer sus funciones de supervisión en este ámbito el principio de proporcionalidad (numerosas ICOs son de volumen pequeño o mediano). Sin perjuicio de las precisiones anteriores, la CNMV considera que buena parte de las operaciones articuladas como ICOs deberían ser tratadas como emisiones u ofertas públicas de valores negociables. Ello con base, entre otras razones, en el amplio concepto de valor negociable contenido en el artículo 2.1 del TRLMV*».

ciertos sectores regulados, como el de las TIC o el de los servicios financieros[50], y muy especialmente en la digitalización de los servicios de pago desde la aprobación de la conocida como PSD2[51]. Esta necesidad se ha generalizado, y no solo, como decíamos, por esa complejidad, sino por la rapidez con la que se están concatenando las novedades en estas materias, la enorme diversidad de aplicaciones y la esencialidad de ambas para la economía productiva. Todo ello hace que la colaboración entre abogados e ingenieros y otros técnicos haya devenido, a nuestro modo de ver, absolutamente esencial.

Cada una de las aplicaciones de la tecnología *blockchain* que antes hemos referido suscita infinidad de cuestiones, y lo hace, sin duda, con distinta forma y alcance desde la perspectiva de cada disciplina jurídica. En el mundo de los activos virtuales, por ejemplo, las preguntas nacen ya incluso sobre su misma naturaleza jurídica, esencial para determinar la regulación aplicable a sus transacciones. ¿Tienen valor fiduciario o deben considerarse una permuta de activos?; ¿una (¿posible?) permuta de bienes inmateriales?; ¿una prestación de servicios? La respuesta que están dando las autoridades, sin embargo, no está siendo coordinada y no siempre parece coherente[52].

En el mundo de los *smart contracts*, las dudas son numerosas y muy diversas. Parece haber consenso en el mundo jurídico acerca de que no son nuevos tipos de contratos, sino solo nuevas formas de instrumentarlos para conseguir su ejecución automática. La ejecución del previo acuerdo de voluntades convertido en código informático es en estos casos automática, sin mediar necesidad de confirmación previa ni, por ende, posibilidad de alterar lo previamente pactado[53]. Las cuestiones que esto supone, en el marco de un Derecho de los contratos que fue ideado para prevenir y gestionar incumplimientos, y no para vivir en la paz contractual, son lógicas. ¿Cómo impedir esa ejecución por cambio de circunstancias? ¿Cómo atender a la mala fe en el cumplimiento? ¿Y a los casos de fuerza mayor? ¿Y a los vicios en el consentimiento? Las preguntas son numerosas, desde luego, aunque no por ello debemos descartar que los llamados contratos inteligentes puedan ser en muchos casos una buena respuesta en sí mismos, o un muy buen instrumento para conseguir o hacer eficientes mecanismos jurídicos para incentivar o asegurar el cumplimiento.

Cualquier disciplina jurídica concreta en la que nos adentremos genera, por lo demás, sus propias cuestiones jurídicas, y también sus oportunidades. Pensando en las que son nuestras áreas personales de trabajo, los ejemplos son particularmente numerosos. Solo por mencionar algunos: ¿es posible estructurar sobre una red construida en código abierto un nuevo negocio que requiere o va a posibilitar desarrollos informáticos que se pretenden privativos y objeto de explotación?; ¿puede el *blockchain* ayudar al seguimiento del cumplimiento de los términos de licencias de derechos de propiedad intelectual?; ¿puede hacerlo en cadenas de distribución?; ¿y en el marco de la utilización de marcas colectivas y de garantía?; ¿qué responsabilidad tendrán los nodos validadores de una red *blockchain* que presta servicios de plataforma a terceros con fines comerciales?; ¿impide realmente la irrevocabilidad que caracteriza esta tecnología cumplir con las distintas obligaciones de no conservación en materia de datos personales?; ¿sus posibilidades técnicas permiten realizar procedimientos de anonimización con las garantías debidas?; ¿pueden protocolos de código abierto cumplir las reglamentaciones sobre seguridad?. Todos estos son solo el principio de una larga lista.

---

50 En relación con la aplicación de innovaciones tecnológicas en los servicios financieros: GARCÍA-OCHOA, David, y PUENTE, Ibai: «Fintech: el futuro de los servicios financieros», *Revista Española de Capital Riesgo*, N.º 1/2017.

51 Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE.

52 En material fiscal, una descripción de las decisiones acaecidas hasta la fecha (en particular, de la Sentencia del TJUE de 22 de octubre de 2015, Skatteverket c. David Hedqvist, asunto C-264/14 y de la Sentencia de la Audiencia Provincial de Asturias de 6 de febrero de 2015, recurso n.º 27/2015) y de sus consecuencias en la aplicación de la normativa tributaria se encuentra en GIL SORIANO, Alberto: «Monedas virtuales: encaje jurídico y control tributario», en *VI Encuentro de Derecho Financiero y Tributario - Tendencias y retos del Derecho Financiero y Tributario*, Documentos de Trabajo XX/2018, Instituto de Estudios Fiscales, Ministerio de Hacienda y Función Pública (pendiente de publicación).

53 TUR FAÚNDEZ, Carlos, cit. *supra*: «*El Smart contract jurídicamente relevante es el instrumento creado para la ejecución automática del contrato legal inteligente e intervendrá, normalmente, como un tercero inexorable que, de producirse un evento para el que esté programado: a) Podrá recibir fondos de la cuenta de un deudor; b) Podrá cobrar automáticamente de la cuenta de un deudor y transferir los fondos a su propia cuenta o a la del acreedor, con o sin intereses […]; c) Podrá retener fondos en su propia cuenta; d) Podrá recibir información sobre cualquier hecho constatable en el fundo exterior y actuar en consecuencia; e) Podrá ordenar que cualquier mecanismo electrónico exterior interconectado al programa: e.i. Se inicie o detenga; e.ii. Se encienda o se apague; e.iii. Se bloquee o desbloquee; f) Podrá ordenar la detención de su propia autoejecución; g) Podrá ordenar su autodestrucción, en cuyo caso jamás volverá a estar operativo en la cadena de bloques*».

Sin perjuicio de la eventual regulación, lo que parece fuera de duda es, como avanzábamos, que nuestro ordenamiento jurídico actual seguirá aplicándose en cualquier caso. Y, a nuestro modo de ver, las cautelas necesarias o las posibles soluciones requeridas por las cuestiones jurídicas que esta tecnología suscita podrán en muchos casos trabajarse desde las distintas configuraciones que la propia tecnología permite, así como, especialmente, desde la propia regulación contractual, en particular la que regirá en cada caso las reglas de acceso, pertenencia y utilización de las redes privadas.

Es evidente que, tanto para lo primero como para lo segundo, el conocimiento de la tecnología, de su modo de funcionamiento y de sus posibilidades es esencial, como esencial es, por consiguiente, la atención al apoyo técnico necesario en nuestra labor de asesoramiento.