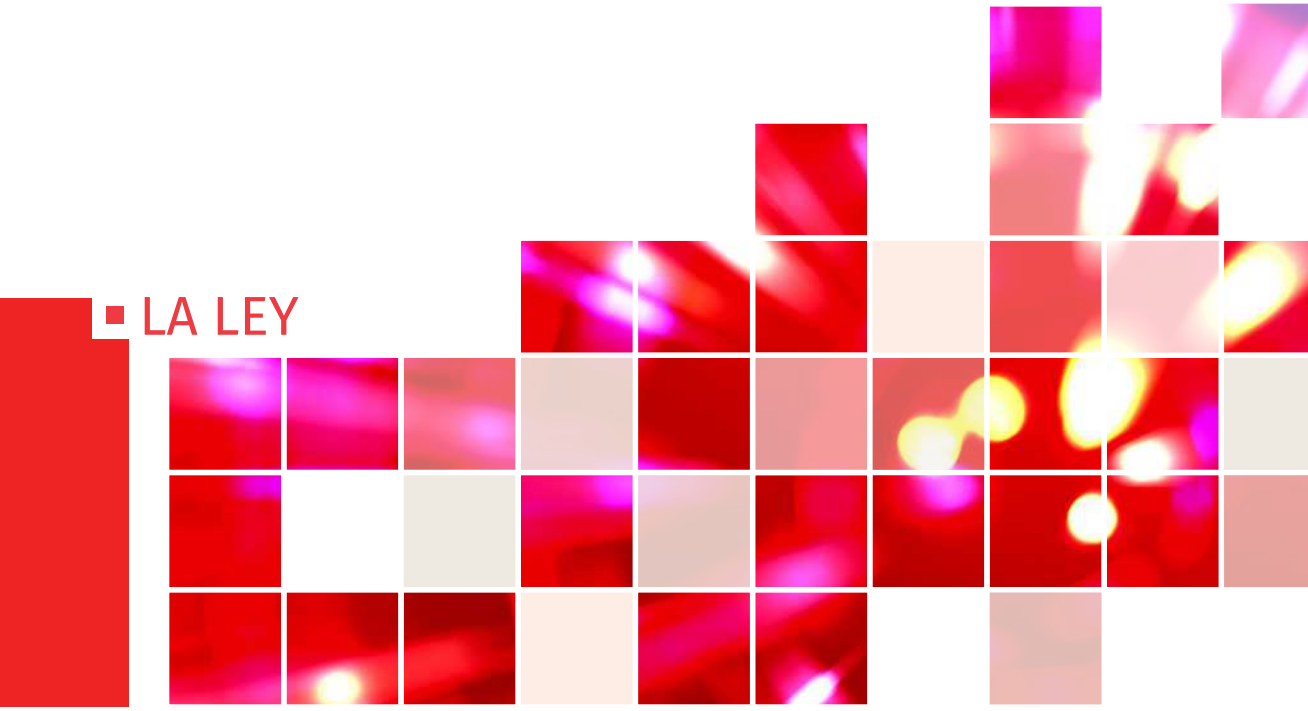
TEMAS

Blockchain: aspectos jurídicos de su utilización

Directores

Eduardo Valpuesta Gastaminza
Juan Carlos Hernández Peña



LA LEY

LA LEY

TEMAS

LA LEY

Blockchain: aspectos jurídicos de su utilización

Directores

Eduardo Valpuesta Gastaminza
Juan Carlos Hernández Peña

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

LA LEY

Wolters Kluwer Legal & Regulatory España
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
http://www.wolterskluwer.es

Primera edición: Mayo 2022

Depósito Legal: M-14565-2022
ISBN versión impresa: 978-84-19032-57-7
ISBN versión electrónica: 978-84-19032-58-4

Diseño, Preimpresión e Impresión: Wolters Kluwer Legal & Regulatory España, S.A.
Printed in Spain

CAPÍTULO I

EL *BLOCKCHAIN* EN SU LABERINTO: *BLOCKCHAIN* PÚBLICAS *VS. BLOCKCHAIN* PRIVADAS, HE AHÍ LA CUESTIÓN (*)

Eduardo Valpuesta Gastaminza
Catedrático de Derecho Mercantil
Universidad de Navarra

(*) Trabajo realizado dentro del Proyecto de Investigación «Problemas jurídicos que plantea el uso de *blockchain*», Ministerio de Ciencia, Innovación y Universidades, referencia RTI2018-100946-B-100, del que es IP el autor.

1. LA TÉCNICA DE LA «CADENA DE BLOQUES» *(BLOCKCHAIN)*

Llevamos ya trece años desde la creación de la técnica de la «cadena de bloques» (*blockchain*), con múltiples aplicaciones y derivaciones de la misma, y todavía para muchas personas, incluso de las dedicadas a estos temas, esta técnica sigue siendo la «gran incomprendida». Y es que, en efecto, salvo que se disponga de conocimientos de computación, la técnica de la «cadena de bloques» como tal no se debe «comprender», sino simplemente «aceptar». Funciona, igual que la transmisión de datos digitales a través de correo electrónico funciona, y podemos ver sus efectos, aunque no tengamos ni idea de la fundamentación tecnológica de esa operativa. Lo que sí resulta preciso, para poder realizar una aproximación desde el punto de vista jurídico, es comprender algunos de sus aspectos, unos puramente pragmáticos (como qué es un *hash*) y otros más estrictamente jurídicos (como la configuración de las identidades, o el alcance de la validación de las operaciones). A esto dedicaremos este primer epígrafe, partiendo de la primera *blockchain*, la de Bitcoin, para luego ver la evolución actual hacia la gran diversidad de «cadenas de bloques» que pueden configurarse. Y siempre teniendo en cuenta que la tecnología avanza de tal manera que cualquier cosa que se escriba, por actualizada que esté, ya resulta obsoleta cuando resulta impresa. Por eso expondremos el fenómeno en sus rasgos esenciales, no con los múltiples matices que puede tener la configuración en un día concreto.

1.1. Cómo comenzó todo: la *blockchain* de Bitcoin

1.1.1. El surgimiento de Bitcoin y su finalidad

La técnica *blockchain* no se originó desde cero, sino que partió de una serie de aportaciones realizadas por técnicos de computación en el último cuarto del siglo pasado. Pero ciertamente la *blockchain* Bitcoin fue la primera formulación definitiva y completa de una manera de alojar datos digitales de

forma descentralizada e inmodificable[1]. Por eso debemos partir de su configuración, para luego entender la evolución que ha experimentado como técnica y como desarrollo.

La cadena de bloques Bitcoin fue creada por Satoshi Nakamoto, nombre que constituye un seudónimo de una o varias personas que prefirieron ocultar su identidad. La teoría la formularon en el famoso *paper*, publicado en octubre de 2008, «*Bitcoin. A Peer-to-Peer Electronic Cash System*». Y la implementación práctica se inició con la primera operación que se incluyó en la *blockchain* Bitcoin: la compra de una pizza, que supuso la primera operación que se alojó en el primer bloque de la «cadena»[2]. Como expresamente se declara en el *paper*, la cadena nació como una forma de lograr un sistema de «pago electrónico» directo entre particulares, sin necesidad de ningún intermediario, ahorrándose los costes dinerarios y temporales y con una seguridad basada en sistemas matemáticos. Bitcoin surgió como una manera de alojar y documentar pagos entre particulares, como una «criptomoneda», aunque actualmente la función de su «moneda», el bitcóin, como medio de pago, no se haya generalizado, y cumpla más bien una función de inversión o especulación. Como se ha señalado repetidamente, Bitcoin es una derivación de dos grupos de ideas que si bien surgieron en ámbitos distintos, resultan afines y complementarios: el «Manifiesto Criptoanarquista» (1992) y la «Declaración de Independencia del Ciberespacio» (1996)[3]. Aquél promovía una emancipación del individuo respecto de los poderes y maquinarias estatales, algo que se podría lograr gracias a la tecnología, a la actuación bajo

(1) Como señalan Narayanan, Arvind – Clark, Jeremy, *Bitcoin's Academic Pedigree*, 2017 (disponible en https://collaborate.princeton.edu/en/publications/bitcoins-academic-pedigree) existen muchos trabajos académicos de cuyos resultados parte Bitcoin, que en este sentido se asentó «sobre hombros de gigantes», pero el diseño de esa primera *blockchain* supuso una novedad al conjugar todos esos avances previos en un sistema completo. Nakamoto no publicó su trabajo como algo científico y en una revista académica, y por eso su trabajo fue minusvalorado por algunos, hasta que se apreció que esa hipótesis funcionaba perfectamente y resolvía múltiples problemas.

(2) El *paper* está disponible en español en https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf. La primera operación se realizó el 3 de enero de 2009, generando el primer bloque por el que se obtuvo la recompensa de 50 bitcoines.
La *blockchain* se denomina Bitcoin, con la B mayúscula, mientras que la moneda se escribe «bitcóin», en minúscula. En la actualización del Diccionario de la Real Academia de la Lengua Española de 2021 ya se ha admitido la voz «bitcóin» (o «bitcoin») como «Moneda digital», por lo que la utilizaremos en adelante sin cursiva, como palabra ya admitida en nuestro idioma (la plataforma «Bitcoin» se sigue citando con la primera letra en mayúscula, y como una marca, por lo tanto, sin tilde ortográfica).

(3) González-Meneses, Manuel, *Entender Blockchain*, Aranzadi, Cizur Menor (Navarra), 2017, págs. 19-28; Carrascosa Cobos, Cristina – Kuchkovsky Jiménez, Carlos – Preukschat, Álex, «Hacktivismo, cypherpunks y el nacimiento de la blockchain», en Preukschat, Álex (coord.), *Blockchain: la revolución industrial de internet*, Gestión 2000, Barcelona, 2017,

identidades anónimas y mensajes cifrados, situación que aún se mantiene en parte con la existencia de la *deep web*; y este proclamaba más bien la independencia del ciberespacio como un lugar sometido a reglas propias, ajeno a las leyes estatales, donde se podía negociar libremente entre identidades electrónicas. Bitcoin constituiría así una economía autónoma e independiente de los poderes estatales, regida por reglas propias, con individuos que controlan el sistema y tienen acceso al mismo de forma directa. Desde luego, las cosas han evolucionado desde aquel surgimiento en 2009, y en la actualidad cabría plantearse si el propio «mercado» de las criptomonedas no constituye un cierto remedo del sistema capitalista, quizás con menos costes, pero posiblemente también con riesgos mucho mayores(4). Y si lo que se pretendía era acabar con los intermediarios, más bien lo que se ha hecho es crear unos intermediarios distintos(5).

Esta primera *blockchain* se caracterizaba por las siguientes notas, de las cuales no todas son comunes a las *blockchain* creadas a partir de la misma. Para exponerlas, partimos de cualquier transacción alojada en esta cadena, que se puede «contemplar» en páginas como https://www.blockchain.com/explorer?view=btc (y de cuyos ejemplos partiremos en la siguiente exposición).

---

págs. 189-195; Ibáñez Jiménez, Javier Wenceslao, *Blockchain: primeras cuestiones en el ordenamiento español*, Dykinson, Madrid, 2018, pág. 40; Arroyo Guardeño, David – Díaz Vico, Jesús – Hernández Encinas, Luis, *Blockchain*, CSIC-Los Libros de la Catarata, Madrid, 2019, pág. 44; Barrio Andrés, Moisés, *Fundamentos del Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020, págs. 150 y ss. En la doctrina extranjera Casey, Michael J. – Vigna, Paul, *The truth machine. The blockchain and the future of everyting*, HarperCollins, Londres, 2018, págs. 17-35; Pejic, Igor, *Blockchain Babel. The Crypto Craze and the challenge to business*, KoganPage, Londres-Nueva York-Nueva Delhi, 2019, págs. 47-71. Sobre la ideología *cypherpunk* puede verse Assange, Julian, *Cypherpunk. Freedom and the Future of the Internet*, OR Books, Nueva York, 2012.

(4) Por otra parte, hay que señalar que actualmente los mercados de criptomonedas pueden influir incluso en la estabilidad del sistema financiero global (ese sistema al que pretendían sustituir, o caminar en paralelo), porque es posible que los fondos de inversión diversifiquen sus inversiones y las realicen en criptomonedas, con lo cual la volatilidad de este mercado se podría extender al financiero capitalista. De ello avisa el Financial Stability Board en su informe *Assessment of Risks to Financial Stability from Crypto-assets*, 2022 (disponible en https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/). Si bien actualmente el volumen de capitalización de las criptomonedas es relativamente bajo, un «entrecruzamiento» de ambos mercados podría tener consecuencias nefastas.

(5) García Mexía, Pablo, «Del ciberderecho al criptoderecho. La criptorregulación», en García Mexía, Pablo (dir.), *Criptoderecho. La regulación de blockchain*, Wolters Kluwer, Las Rozas (Madrid), 2018, págs. 92-94, pone de relieve cómo la tecnología *blockchain* no sólo puede que no evite la pervivencia de los intermediarios, sino que además añade otros intermediarios nuevos a todo el proceso, como los mineros, los que cambian moneda *fiat* por criptomonedas, las plataformas de cotización, los *wallets*, etc., y refuerza incluso el poder de otros intermediarios ya existentes como los que proveen acceso a internet.

1.1.2. La forma de identificar a los sujetos

La *blockchain* Bitcoin opera con identidades de sujetos que son seudónimas o, en buena medida, anónimas. Si se abre cualquier «transacción» dentro de un bloque, veremos que se produce entre dos «direcciones bitcóin», las cuales se expresan mediante 34 caracteres del lenguaje Base58[(6)]. Cada «dirección bitcóin» designa a un sujeto, persona física o jurídica, pero además cada sujeto puede abrir tantas direcciones bitcóin como desee, de forma que no cabe asemejarlas a una «identidad digital unívoca». Por decirlo de alguna manera, estas «direcciones» son algo parecido a los números de cuenta corriente de cualquier entidad de crédito, una forma de identificarse a la que se adscribe un «saldo» de bitcoines no gastados.

Para la propia Bitcoin, puede que la identidad del «titular» de esa «dirección bitcóin» sea anónima o seudónima. Será lo primero si esa cuenta ha sido creada por algún intermediario que, él sí, puede (y debe, según la legislación a la que esté sometido) conocer la identidad del sujeto, pero no la comunica a Bitcoin (entre otras razones, porque Bitcoin ni le pide esa identidad, ni le importa). Será seudónima si el sujeto abrió directamente la «dirección bitcóin» aportando su identidad, y por lo tanto Bitcoin puede acudir a los datos de registro para conocerla. Pero, en cualquier caso, lo que figura en la *blockchain* no es una identidad de persona física o jurídica, sino una dirección expresada en números y letras.

Esta forma de operar facilita mucho las operaciones, porque todas las identidades tienen igual extensión y una composición parecida, los datos de identificación real no figuran en cada transacción, la identidad del sujeto no es relevante para la operativa de la *blockchain*, etc. Pero, ciertamente, también ampara ciertas actuaciones no transparentes, y por eso uno de los estigmas de este tipo de cadenas es que alientan operaciones de blanqueo de capitales, financiación del terrorismo, o actividades ilícitas, al no figurar ni controlarse la identidad de los sujetos. El sistema nació con una finalidad económica, facilitar pagos transnacionales, y por eso prescindió de aspectos que para un jurista son esenciales, como el control de la identidad (y de, entre otras características, la capacidad de obrar) de los sujetos que realizan las operaciones.

(6) El lenguaje Base58 tiene como caracteres las letras mayúsculas y minúsculas y los números arábigos decimales, excluyendo las que puedan dar lugar a confusión (0 y O, por ejemplo). Suele ser, por ejemplo, el lenguaje usado para identificar a los *Router* de nuestros sistemas *wifi*.

Por otra parte, para operar con esas «direcciones» el sistema parte del sistema de la llamada «criptografía asimétrica»: al generar una dirección bitcóin, el sistema crea dos claves o números. El primero de ellos es la llamada «clave pública», la «dirección bitcóin» que vemos cuando leemos cualquier transacción. El segundo número es la clave privada, que sólo conoce el titular, y que debe mantener en secreto. El titular puede transmitir su clave pública a un tercero (por ejemplo, para que este tercero le transmita bitcoines), y utiliza su clave privada para cifrar sus mensajes (que opera, así, de modo muy parecido a una «contraseña»). Para realizar operaciones con los fondos que tiene en la dirección pública, utiliza la clave privada, y de esta forma el sistema se asegura de que todas las operaciones han sido consentidas por el titular (únicamente él dispone de la «contraseña»)[7]. Las claves públicas lo son en la medida en que se pueden comunicar a otros, o podemos verlas en una *blockchain*, pero no existe un «listado de claves públicas» que nos diga, por ejemplo, quien es el titular. El sistema sigue siendo anónimo o seudónimo, porque Bitcoin ni tiene ni (por ello mismo) proporciona ninguna correlación de claves públicas con titulares. Como afirmábamos en el párrafo anterior, a Nakamoto no le interesaba controlar identidades, sólo generar un sistema confiable y seguro de transmisión «de particular a particular».

1.1.3. La encriptación de las operaciones mediante hashes

Por razones operativas, entre otras, una *blockchain* normalmente no constituye un repositorio o un alojamiento de documentos. Podría serlo, pero eso precisaría de mucho más «espacio virtual» de almacenamiento, y además tendría el problema de posibles accesos ilegítimos a los documentos alojados. Por eso Bitcoin opera con una especie de «resúmenes» de la transacción o documento que aloja. Pero para hablar de esos resúmenes es preciso aludir a una institución o concepto que es el «*hash*».

El *hash* es el resultado de encriptar, de cifrar, un documento (una hoja escrita, una foto, un libro entero) para hallar un número que tiene la característica de que, a partir del documento se obtiene el *hash*, pero a partir del

(7) Sobre el uso de criptografía en internet, con consideraciones interesantes para este y otros apartados de este trabajo, véanse Fúster Sabater, A. *et alii*, *Criptografía, protección de datos y aplicaciones. Una guía para estudiantes y profesionales*, RA-MA, Madrid, 2012; Hernández Encinas, Luis, *La criptografía*, CSIC-Los Libros de la Catarata, Madrid, 2016; Núñez Miller, Jaime, «Criptografía y consenso aplicado a la blockchain», en Preukschat, Álex (coord.), *Blockchain: la revolución industrial de internet*, Gestión 2000, Barcelona, 2017, págs. 203-22; Chaum, David, «Blind Signatures for Untraceable Payments», *Advances in Cryptology. Proceedings of Crypto 82*, Springer, Boston, 1983, págs. 199-203; Zimmerman, Phil, «Cryptography for Internet», *Scientific American*, 1998, disponible en https://philzimmermann.com/docs/SciAmPRZ.pdf

El *blockchain* o «cadena de bloques» constituye una tecnología que permite tratar y alojar datos digitales de forma no modificable en una base de datos compartida por multitud de nodos. Si bien se utilizó inicialmente, a partir de 2009, para trazar las transacciones de criptomonedas (al principio de bitcoines, pero luego de otros muchos criptoactivos), actualmente tiene aplicaciones en numerosos ámbitos negociales (contractuales, financieros, societarios, etc.) y sociales (alojamiento de datos tomados por drones, operativa de *smart cities*, procesos electorales, etc.). Como solución tecnológica es innegable que ha supuesto una verdadera revolución en los mecanismos de alojamiento de datos, pero se echa en falta un desarrollo normativo que otorgue seguridad y eficacia jurídica a esta tecnología.

Esta monografía expone las características fundamentales de la tecnología *blockchain,* los intentos de regulación, el sometimiento a la normativa de protección de datos personales, y diversas aplicaciones de la misma en el ámbito jurídico: *non fungible tokens* (NFTs), *smart contracts*, ejercicio de derechos del socio, trazabilidad de políticas socialmente responsables, valor probatorio, utilización de drones, y ejercicio del derecho de voto en elecciones. En cada uno de estos aspectos se resaltan los problemas jurídicos fundamentales que se plantean y el marco normativo general al que acudir para solucionar las controversias que surjan entre los sujetos que utilizan una *blockchain*.

ISBN: 978-84-19032-57-7

9 788419 032577 3652K61504

AENOR ER Empresa Registrada ISO 9001 ER-0280/2005

IQNet

AENOR GA Gestión Ambiental ISO 14001 GA-2005/0100

LA LEY