# Descifrando la blockchain

**ACTUALMENTE SE ESCUCHAN CON FRECUENCIA TÉRMINOS COMO BLOCKCHAIN, BITCOIN, FINTECH, CRIPTOMONEDAS Y MUCHOS MÁS, PERO LA MAYORÍA DE LOS CIUDADANOS SIGUEN SIN ENTENDER QUÉ SON Y QUÉ IMPORTANCIA TIENEN. ESTE ARTÍCULO TRATA DE AYUDAR A ENTENDERLOS MEJOR.**

A medida que el precio del bitcoin empezó a escalar y su notoriedad lo ubicó en el foco de atención del mundo financiero, la palabra *blockchain* empezó a popularizarse. En muchas revistas, blogs y prácticamente cualquier medio de comunicación se ha intentado explicar el concepto; sin embargo, el funcionamiento de la *blockchain* sigue siendo incomprendido por la mayoría de las personas, incluso aquellas que participan activamente de la red.

Una *blockchain* es un conjunto de nodos que, conectados a una red descentralizada, utilizan un protocolo estándar con el objetivo de validar y almacenar la misma información registrada en una red P2P, de forma que todos podamos intercambiar bienes y servicios sin necesidad de terceros. Dicho de otro modo, una *blockchain*, también conocida como cadena de bloques, es una tecnología que permite mantener una base de datos distribuida entre una red de ordenadores. Esta información está asegurada por el mismo hecho de estar distribuida por todo el sistema, evitando así que esta sea modificada sin el consentimiento del resto de ordenadores. Esta tecnología está surgiendo con tal fuerza que muchos la comparan con el surgimiento del internet.

**Una blockchain, también conocida como cadena de bloques, es una tecnología que permite mantener una base de datos distribuida entre una red de ordenadores**

## ORIGEN Y ASPIRACIONES

Con el crecimiento exponencial de las nuevas tecnologías, han surgido en los últimos años diferentes movimientos que buscan una nueva forma de relacionarse en internet reinterpretando conceptos como los de información, libertad y confianza. Entre esa clase de movimientos destacan los hacktivistas y los cypherpunks. Son esos movimientos los que, entre otros, dan origen en 2009 a la primera "*blockchain*" o "cadena de bloques": el origen del ahora famoso *bitcoin*. Tras esta tecnología, se encierra en el fondo la aspiración de facilitar una comunicación segura entre personas de diferentes países, defender la libertad de expresión y evitar el control de los diferentes gobiernos. Debe notarse que la *blockchain* no es un mero internet modernizado, sino que apunta a un radical cambio de paradigma. El internet que se utiliza hoy en día, al que podemos llamar "Internet de la Información", fue creado sobre estándares abiertos, lo que posibilita la libre circulación de información en todo el planeta (salvo en los países donde se encuentra restringido). Esto ha originado un cambio en la forma de relacionarse, trabajar, comprar, entretenerse, etc. Así como la creación de multitud de nuevos modelos de negocio; basta ver el tremendo impacto de empresas como Google, Amazon o Facebook.

Por contraposición al internet de la información, a la *blockchain* se la conoce como el "Internet del Valor". También creada sobre estándares abiertos, sirve para compartir y gestionar el valor de diferentes activos y bienes digitales sin la necesidad de depender de una entidad de confianza que centralice el proceso. Los expertos han definido esta realidad como un nuevo patrón basado en la descentralización de la confianza, donde todos podremos intercambiar bienes y servicios sin necesidad de terceros. En esta definición podemos encontrar los tres elementos básicos que definen una cadena de bloques: confianza, descentralización y ausencia de intermediarios. Al igual que en nuestra realidad diaria, el fundamento de la *blockchain* reside en un elemento necesario también en las relaciones personales: la confianza. En las transacciones ordinarias entre dos partes recurrimos a una tercera que verifique la identidad de ambos agentes. Esto ha creado una extensa red de intermediarios, lo cual tiene sus inconvenientes: posesión y comercialización de información personal, restricción de la privacidad y de las libertades.

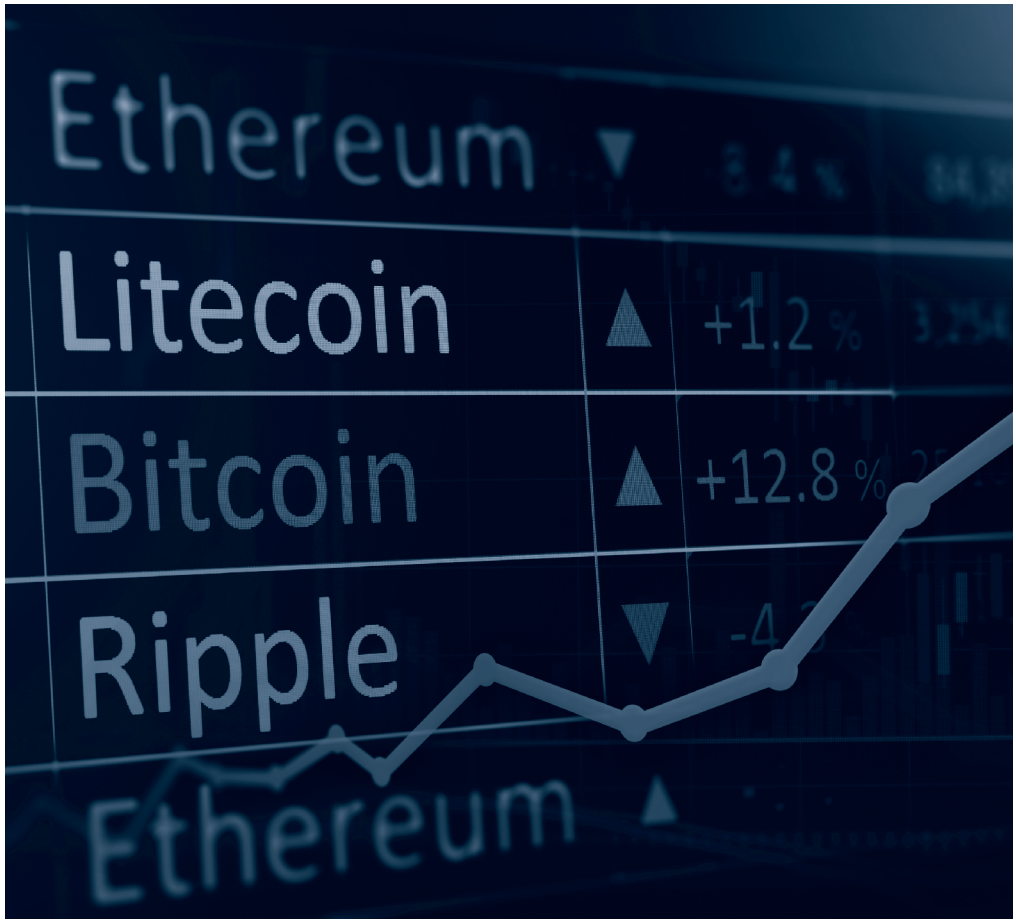
Debido a la corrupción demostrada por numerosos gobiernos y a las prácticas de desinformación cada vez más frecuentes en diversas platafor-

mas y medios (*fake news*), se está popularizando desconfiar de las instituciones. Por ello algunos autores insisten en la necesidad de reconstruir las relaciones de confianza antes de recurrir a soluciones basadas en la tecnología. No obstante, a día de hoy existen multitud de operaciones, con grados de complejidad cada vez más elevados, cuya consecución exitosa no puede depender únicamente de la confianza interpersonal, sino de otros factores derivados principalmente del concepto de seguridad.

Cuando hizo su aparición en 2009, a la *blockchain* no le faltaron opositores que denunciaban la ausencia de una verdadera funcionalidad dentro del marco de la legalidad. Sin embargo, son numerosos los ejemplos tecnológicos que han tenido un recorrido similar al que está viviendo ahora la cadena de bloques, desde los ordenadores hasta los más modernos smartphones. Por eso, muchos empresarios afirman que la *blockchain* ha venido para quedarse. Esta tecnología representa ya toda una revolución en cuanto a la transmisión y gestión del valor de los datos en internet.

### ¿QUÉ UTILIDAD TIENE?

Hoy en día disponemos aún de una visión muy limitada de las posibilidades que puede llegar a ofrecer la *blockchain*. Aunque principalmente, y más ahora con el auge de las criptomonedas, se entienda su uso para el registro de transacciones monetarias, se desconocen muchas otras potenciales aplicaciones. Por lo tanto, es interesante mostrar la infinidad de posibilidades que podría aportar a los diferentes sectores, no solamente económicos, sino también laborales, sociales e incluso militares, como sucedió con internet.




**Por contraposición al internet de la información, a la blockchain se la conoce como el "Internet del Valor"**

En el sector económico, el sistema *blockchain*, más allá de las criptomonedas, ofrece la posibilidad de eliminar cualquier entidad bancaria intermediaria que podría entorpecer e incluso echar para atrás a gran cantidad de inversiones. Por lo tanto, la eliminación de estos intermediarios y sus costes asociados provocaría una mayor exposición del público a la inversión, al tratarse de un sistema que conecta directamente al comprador con el vendedor. De hecho, mercados de valores como el NASDAQ han comenzado a utilizar la *blockchain* en transacciones con valores privados. Debido a esta nueva estructura revolucionaria, recientemente el 80% de los bancos han reconocido que están trabajando en el desarrollo de una tecnología *blockchain* aplicable a su sector.

Sin embargo, las aplicaciones de la tecnología *blockchain* no se limitarán al sector financiero, sino que se están buscando formas para introducirlo en otros sectores en un futuro no muy lejano, al igual que ocurrió con internet. Por ejemplo, en lo que concierne al sector del registro y almacenamiento de datos, esta tecnología permite guardar datos y archivos en una red Peer to peer (P2P), lo que posibilita la distribución de datos de una manera más segura y eficaz. La *blockchain* podría, por lo tanto, llegar a sustituir a plataformas como Dropbox o Google Drive. Asimismo, se ha de tener en cuenta la veracidad de dichos datos, para lo que la cadena de bloques permitiría una verificación instantánea de esos datos compartidos. Adicionalmente, los servidores

DNS (Domain Name Servers) se encuentran actualmente bajo el control de gobiernos y grandes empresas. Los usuarios son por tanto vulnerables a un abuso de poder por parte de estos controladores. El uso de la *blockchain* en este sector permitiría que los DNS se mantuvieran de forma descentralizada, permitiendo que cada usuario tuviese el mismo listado de DNS en su propio ordenador.

El sistema *blockchain* podría llegar incluso al mundo de la política, mediante el voto a través de la red. La cadena de bloques, para ser efectiva, debe asegurar que una persona no pueda votar más de una vez en unas mismas elecciones, al tiempo que garantiza el anonimato de la misma. Un factor importante en este apartado es que al no haber una autoridad central que gestione la votación, no es posible manipularla. En consecuencia, se evita cualquier tipo de amaño en las próximas elecciones de cada país. Además de esto, a los usuarios-votantes se les permite crear su propio perfil, a prueba de cualquier manipulación externa, evitando así la suplantación de identidades. En consecuencia, se eliminaría el tradicional sistema de "usuario-contraseña", muy fácil de hackear por cualquier internauta medianamente hábil.

Por último, se ha de tener en cuenta las capacidades de dicho sistema en lo que respecta a la seguridad individual y pública. La *blockchain* posibilitará la creación de sistemas de seguridad automatizados que permitan o impidan el acceso de determinadas personas de forma completamente automática, facilitando así la labor de las autoridades. Se ha de destacar también el uso militar de la tecnología *blockchain*, ya puesta en marcha por organizaciones internacionales como la OTAN. El DARPA (Defense Advanced Research Projects Agency), por ejemplo, quiere aprovechar esta tecnología para crear un sistema de mensajería seguro. Otra iniciativa en este ámbito es utilizar el sistema para bloquear y desbloquear automáticamente armas y vehículos militares dependiendo de quién trate de manejarlos.

En conclusión, esta nueva estructura informática tiene mucho que aportar a la sociedad. Sin embargo, al mismo tiempo podría generar consecuencias menos deseables. Es por ello de vital importancia la separación entre las ventajas y desventajas de la implantación de dicho sistema.

## IMPLICACIONES POSITIVAS

Confidencialidad. El *bitcoin*, así como otras monedas virtuales, utiliza monederos virtuales que no están asociados a ninguna entidad concreta, por lo que las transacciones son anónimas e irrastreables por parte de Gobiernos y vendedores de información personal. Es importante mencionar que, al referirnos a la confidencialidad y anonimato de las cadenas de bloques, estamos focalizando nuestro estudio en un tipo de *blockchain* más concreta, la pública. En este tipo de redes no se necesitan permisos para participar o volcar información, es decir, son anónimas. Su procedimiento de certificación de nueva información en la cadena se realiza a través de la minería de datos.

**En el sistema blockchain no existe una jerarquía, nadie está por encima de nadie; todos somos iguales.**

## SEGURIDAD

Las operaciones que se registran en la *blockchain* ya no tienen vuelta atrás. Una vez que se agregan son inalterables, porque la información de la operación se replica en todos los nodos y cambiarla en alguno de ellos sería muy sospechoso. Además, se ha de recalcar el complejo sistema de verificación a través de la minería que reduce casi a cero cualquier tipo de hackeo o robo de identidad. Los cambios se podrían hacer, pero se necesitaría el consenso de la mayoría de nodos. La naturaleza de la *blockchain* protege la información de los bloques frente a hackers, que para modificarlos tendrían que convencer a todos y cada uno de los nodos. Por esto se convierte en un sistema muy resistente a ataques, fallos o falsificaciones. Además, al encontrarse al mismo nivel, si uno de estos bloques es hackeado o alterado no pondría en peligro a todos, por lo que la fuerza de la *blockchain* radica así en la unión de los usuarios ("la unión hace la fuerza").

## AHORRO DE COSTES

La tecnología *blockchain* aprovecha los avances en software, comunicaciones y encriptación para soportar un registro digital compartido de transacciones registradas y verificadas a través de una red de participantes. Al ser los propios miembros de la *blockchain* los que verifican estas transacciones, las diferentes empresas, especialmente los bancos, podrían reducir sus costes en el procesamiento de datos, archivo de información, validación de operaciones... Hoy en día, para completar cualquier transacción, las entidades finan-

cieras deben verificar y confirmar sus datos con sus clientes, un proceso complejo y costoso, y que requiere una gran cantidad de mano de obra. Por tanto, los costes asociados a los intermediarios y terceros verificadores de las operaciones podrían ser prácticamente suprimidos. Además, podrían también reducirse costes como el de los informes financieros, como resultado de la optimización de la calidad de los datos, así como la transparencia y los controles internos proporcionados con una fuente compartida y única de datos verificados. Podrían suprimirse también los costes de cumplimiento, debido a una mayor transparencia de las transacciones, además del ahorro que podría suponer el establecimiento de procesos más eficientes para gestionar identidades digitales y compartir una única fuente de datos de clientes de forma segura a través de múltiples bancos.

### DEMOCRATIZACIÓN

El hecho de que la *blockchain* no tenga un núcleo central por el que pasa toda la información hace que todos sus usuarios estén al mismo nivel. De esta forma, se evita cualquier tipo de abusos que podrían ser ocasionados por grandes empresas o Gobiernos. En el sistema *blockchain* no existe una jerarquía, nadie está por encima de nadie; todos somos iguales.

### IMPLICACIONES NEGATIVAS

Evidentemente, "no es oro todo lo que parece". Las bondades de la *blockchain* se ven contrarrestadas por una serie de dificultades y puntos negativos, la mayoría de ellos como consecuencia de tratarse aún de una red novedosa y poco utilizada, que hace que se deban revisar algunos de sus principios si queremos que pueda de verdad convertirse en el "internet del futuro".

**Uno de los mayores problemas de la blockchain procede precisamente de uno de sus "puntos fuertes": el anonimato**

### ANONIMATO

Uno de los mayores problemas de la *blockchain* procede precisamente de uno de sus "puntos fuertes": el anonimato. Es cierto que el anonimato es una fuente de seguridad, al impedir el hackeo y la posibilidad de conocer los datos e información confidencial de cualquier transacción que se realice a lo largo del planeta. Sin embargo, esta circunstancia, llevada al extremo, no hace más que generar dificultades y problemas. Con el nacimiento del bitcoin en 2009, muchos fueron los que alabaron el anonimato que producía esta nueva moneda virtual. La posibilidad de realizar transacciones sin la necesidad de un órgano central controlador que pudiese "espiar" nuestros movimientos hizo que muchos ciudadanos de numerosas nacionalidades viesen en esta moneda una posibilidad de evasión y de libertad. Al poco tiempo, no obstante, comenzaron a surgir los primeros problemas. La imposibilidad del rastreo en las *blockchain* hizo que numerosas páginas en la *Deep web*, como la famosa *SilkRoad* (cerrada por la Justicia Norteamericana en 2013) aceptasen bitcoins a cambio de drogas, servicios de hackeo, robo de cuentas, asesinatos... La criptografía utilizada provocaba un anonimato que hacía imposible que el Gobierno o cualquier institución jurídica pudiesen rastrear el origen de estas transacciones, siendo inútil el intento de juzgar y castigar dichos crímenes.

Mercados como estos siguen existiendo en la *Dark Web* (la parte más interna de la *Deep Web*, en donde es prácticamente imposible ningún tipo de rastreo), pero podríamos afirmar que las garantías que ofrecen la *blockchain* o el bitcoin están muy lejos de las que pueden llegar a ofrecer bancos y Gobiernos, al basar las transacciones realizadas en la verificación de las personas implicadas en la misma. Por lo tanto, esto también minimiza los riesgos de que las divisas de curso legal se utilicen para financiar cualquier tipo de delitos, algo que, como ya hemos visto, es mucho más complejo de controlar en las cadenas de bloques.

Aun así, no está demostrado que exista un anonimato absoluto dentro de las *blockchain*. Un estudio publicado por investigadores de la Universidad de Qatar7 afirmó haber podido revelar la identidad de los clientes de sustancias ilícitas en *SilkRoad* en al menos 22 de las 100 direcciones IP analizadas, a partir del sistema de trazabilidad de la misma *blockchain*. El estudio también pudo detectar diferentes operaciones llevadas a cabo en Wikileaks, Snowden Defense Fund, The Pirate Bay y otros sitios dentro de la *Deep Web*.

### VULNERABILIDAD

Otro de los pilares sobre los que se asienta la *blockchain* es la supuesta seguridad que ofrece esta tecnología. Aunque es cierto que las cadenas de valores son de las tecnologías más seguras en la actualidad, aún hay que dar muchos pasos si queremos lograr la seguridad completa y sin riesgos. La mayoría de los problemas de seguridad de las

*blockchain* derivan, sin embargo, de su reciente introducción y de su novedad. Los programadores, y mucho menos los ciudadanos, no dominan aún del todo esta tecnología, lo que provoca desconocimiento e ignorancia a la hora de llevar a cabo simples transacciones. Una de las principales vulnerabilidades procede de los anteriormente mencionados *Smart Contracts*, o Contratos Inteligentes, y su dificultad en el uso normal para las personas de a pie. El propio diseño y arquitectura de la red *blockchain* es también una fuente de conflictos, en especial en las redes más noveles y aquellas vinculadas a personas individuales, lo que hace que sean más sencillos ataques como el *phishing* (suplantación de identidad). Las personas atacadas son analizadas durante meses, utilizando técnicas de inteligencia para recabar información y lanzar un ataque personalizado para poder así obtener los diferentes datos de la víctima.

**El impacto que está produciendo este nuevo modelo económico y social basado en la lógica de las cadenas de bloques guarda una estrecha relación con el surgimiento del internet que conocemos hoy en día**

## LA BURBUJA

Otro tema preocupante, especialmente tras lo visto en los últimos meses, es la similitud entre la situación actual de las *blockchain*, especialmente en lo relacionado con las criptomonedas o monedas virtuales (y muy particularmente las *bitcoin*) y la burbuja de las *dotcom* a finales de los años 90 y principios de los 2000. La especulación y la volatilidad en torno a estos productos están poniendo en duda su desarrollo.¿A qué se debe esta burbuja? Las razones no están claras del todo, pero podríamos decir que la causa principal de esta impresionante montaña rusa de precios es la generación de altas expectativas por parte de los ciudadanos. La especulación con toda empresa o moneda que utilice las *blockchain* es muy similar a la vivida hace quince años. Las expectativas generadas provocan que el precio de las acciones de las compañías que utilizan la *blockchain* siga subiendo cada vez más, llegando a niveles de enorme riesgo. La burbuja creada con las *dotcom* y, más recientemente, con las *bitcoin* no hace más que augurar un destino aciago para muchas de estas compañías. Compañías, además, que invierten una gran cantidad de capital en el desarrollo de estas tecnologías (se estima que solamente en energía para activar los procesos de minería se llegan a gastar más de 400 millones de dólares al año) y que podrían ir a la quiebra si la burbuja finalmente explota.

## CONCLUSIONES

En resumen, podríamos afirmar que la *blockchain* es una tecnología que va a cambiar el futuro. Para que de verdad pueda llegar a conseguirlo y hacer que convivamos en una sociedad más segura y a la vez más libre es necesario, sin embargo, que se den ciertos cambios.

Como ya se ha explicado, el impacto que está produciendo este nuevo modelo económico y social basado en la lógica de las cadenas de bloques guarda una estrecha relación con el surgimiento del internet que conocemos hoy en día. La *blockchain* surgió como un mercado paralelo al Internet de la Información, pero con unas “reglas de juego” diferentes. Los contrastes fundamentales entre la *blockchain* y

el mercado actual son la descentralización y la confidencialidad que, llevadas al extremo, pueden dar lugar a problemas legales y morales. En el mercado del internet actual, existen ciertas instituciones que establecen reglas derivadas del principio de justicia. En el nuevo mercado de la *blockchain*, sin embargo, no existe ninguna entidad reguladora del sistema, lo que puede acarrear una serie de dificultades a la hora de organizar la masiva red de transacciones que se pueden dar en el mercado.

Donde hay intercambios, rigen los principios de la justicia conmutativa, al venderse los diferentes productos al precio que cada uno considera "adecuado". Rige también la ley de la oferta y la demanda, en la que los bienes serán vendidos y comprados cuando ambas partes estén satisfechas con el acuerdo, es decir, cuando les parezca justo. Llamamos justo a aquel que, en los conflictos de intereses, examina de qué intereses se trata y está dispuesto a pasar por alto de quién son los intereses que están en liza. Lo que hace que se tenga medida de lo justo son la experiencia y, muy especialmente, la comunicación, caracteres que no se dan de manera evidente en la *blockchain*.

Esta situación provocará, a medio plazo, que se puedan llegar a cometer injusticias generalizadas dentro de la cadena de bloques. Los usuarios más experimentados y capacitados podrían aprovecharse de la ignorancia de los ciudadanos "de a pie", que reclamarán a los poderes públicos la regulación y control de redes como éstas. Estas personas comenzarán por tanto a crear diferentes normas e instituciones reguladoras de una tecnología que supondrá una de las claves fundamentales del Estado de Bienestar, como actualmente lo es internet. En ese momento empezarán a regir los principios de la justicia distributiva (la correcta distribución de los bienes escasos en la Economía), entre los que se encuentra el principio de libre asociación.

**Es probable que siguiendo un proceso natural de mercado, y gracias a esa futura regulación del sistema, la blockchain se acabe pareciendo al Internet de la Información, del que en un principio quería desligarse**


Es probable que, siguiendo un proceso natural de mercado, y gracias a esa futura regulación del sistema, la blockchain se acabe pareciendo al Internet de la Información, del que en un principio quería desligarse. Procesos como éste se han dado en numerosas ocasiones a lo largo de la historia económica, y cabe pensar que, quizás en unos años, estaremos hablando del fin de la *blockchain*, y del comienzo de una nueva tecnología, de algún nuevo sistema innovador y mucho más eficaz que pueda resolver de manera eficiente los problemas a los que se enfrentará la sociedad del futuro. Pero mientras tanto, es bueno aprender lo que sea necesario de las bondades y los problemas de un desarrollo tecnológico con tanto potencial como el de las cadenas de bloques.

CARLOS MITRE ABUHAYAR, JESÚS ALONSO-ALLENDE, MARÍA ESCAURIAZA, JAVIER GONZALO, RICARDO MÁRQUEZ, FRANCISCO JAVIER MORENO