4. Descifrando la *blockchain:* qué es y cómo nos puede afectar*

Actualmente se escuchan con frecuencia términos como *blockchain*, *bitcoin*, *fintech*, criptomonedas y muchos más, pero la mayoría de los ciudadanos seguimos sin entender qué son y qué importancia tienen. Este artículo quiere ayudar a entenderlos mejor.

A medida que el precio del *bitcoin* empezó a escalar y su notoriedad lo situó 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 este concepto, sin embargo, el funcionamiento de la *blockchain* sigue siendo incomprendido por la mayoría de las personas, incluidas aquellas que participan activamente de la red.

¿Qué es la *blockchain*?

Una *blockchain* es una base 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 descentralizada, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Sirve para registrar cualquier tipo de información, comprimirla, cifrarla y transmitirla. 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.

*Publicado en Nuevas Tendencias, nº 100 (2018) , pp. 33-38.

Origen y aspiraciones

La *blockchain* tiene aún un enorme camino que recorrer en los próximos años. Por eso, hemos ido un paso más adelante y nos disponemos a explicar las implicaciones, tanto positivas como negativas, de esta tecnología que en el futuro puede llegar a cambiar la forma en que compartimos, organizamos y protegemos información de gran valor.

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 la información, la libertad y la 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 en todo el planeta (salvo en los países donde se encuentra restringido) de la información. 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.

Internet de la información versus Internet del valor

Por contraposición al internet de la información, la *blockchain* es conocida 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 de-

finido 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 intermediaries. 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 plataformas 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 afirmaban 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 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 valor de los datos en internet.

¿Qué utilidad tiene?

Todavía tenemos una vision 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. El verdadero potencial no está en esa u otras monedas digitales, sino en la tecnología que está detrás de todas ellas, la *blockchain* 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.

Ciertamente, al igual que sucedía en los comienzos de lo que ahora conocemos como internet, el soporte de la *blockchain* encierra una alta complejidad técnica. En este artículo haremos algunas referencias a su funcionamiento, pero sin ánimo de entrar a fondo en el diseño informático que lo sustenta, dado que no es nuestro objetivo.

¿Cómo funciona? *Bitcoin:* la punta del iceberg

Para empezar, es necesario tener claro que *blockchain* no es lo mismo que *bitcoin*. La *blockchain* es una nueva tecnología que, como hemos comentado, sirve para compartir y gestionar el valor de activos o bienes digitales sin la necesidad de depender de una entidad central intermediaria de confianza que regule el proceso. En cambio, *bitcoin* es una criptomoneda que funciona *mediante* el uso de una *blockchain*. Existen muchas criptomonedas, siendo aún el *bitcoin* la más importante,

Su creador, el desconocido Satoshi Nakamoto, publicó en 2008 un artículo en el que describía un sistema Peer-to-Peer -entre pares- y un protocolo de dinero digital. De esta manera comenzaba una nueva revolución digital.

El intermediario como garante de operaciones

Los sistemas de pago que hasta ahora conocemos requieren de intermediarios o terceros que verifican que el pago se realiza sin ningún inconveniente, cobrando una comisión por ello. Actual-

mente existen tecnologías para realizar pagos, muy variadas y unas más modernas que otras, como la tarjeta de crédito o de débito. Éstas llevan ya muchos años funcionando y, pese a que siguen mejorando, su esencia sigue siendo exactamente la misma: un sujeto posee una cuenta en un banco con una cantidad determinada de dinero. Para realizar un pago, el sistema de la tarjeta (Visa, MasterCard, entre otros) verifica que la tarjeta sea válida, que la compra esté aceptada (firma o PIN) y que la cuenta cuente con los fondos suficientes, para posteriormente aceptar la transacción. En todo el proceso los sujetos que envían dinero no tienen control alguno sobre su desarrollo, ya que es el banco quien se encarga de hacer que el dinero pase de una cuenta a otra.

Los actores de la *blockchain*

Una *blockchain* es una cadena de bloques de información -bloques que se enlazan de forma sucesiva, como una cadena-. Está diseñada para que no sea posible su modificación una vez que los datos han sido publicados utilizando un sellado de tiempo confiable. Además, el bloque en cuestión se encuentra enlazado al bloque inmediatamente anterior.

La red está compuesta por nodos. Estos nodos son el elemento principal de la red y son, básicamente, cualquier ordenador. Todos éstos deben poseer el mismo protocolo para comunicarse entre sí, y pueden ser anónimos o con nombre, dependiendo de si se trata de una red pública o privada. La principal diferencia entre ambas redes radica en el acceso y visualización de la información, libre en el caso de las redes públicas y restringido en las privadas.

El protocolo que permite a los ordenadores comunicarse entre sí es un software informático que otorga un estándar común para definir la comunicación entre los ordenadores participantes de la red. Para que la información pueda ser transmitida entre los nodos, es necesario una red entre pares o P2P (Peer-to-Peer, en inglés). Finalmente, se requiere un sistema descentralizado en el que todos los ordenadores que están conectados a la red son iguales entre sí.

No hay ninguna jerarquía entre los nodos, por lo menos en una red pública, aunque puede haberlo en las privadas.

Por tanto, una *blockchain* se define como "un conjunto de ordenadores (nodos) que, conectados a una red descentralizada, utilizan un mismo sistema de comunicación (el protocolo) con el objetivo de validar y almacenar la misma información registrada en una red P2P".

Una *blockchain* se compone de varias partes esenciales que al combinarse e integrarse cumplen un propósito determinado y fundamental, que variará en función del ámbito de aplicación de la cadena de bloques. Las claves de la tecnología son la criptografía, la cadena de bloques en sí y un protocolo de verificación. Habiendo explicado ya la necesidad de un protocolo de verificación para un correcto funcionamiento de la *blockchain*, pasamos ahora a desarrollar una brevísima explicación -debido a que su alta complejidad exigiría mucho más de lo que abarca este trabajo- de las otras dos claves de esta tecnología: la criptografía y la morfología de la cadena de bloques.

Criptografía

La criptografía es la clave fundamental que garantiza la seguridad dentro de una *blockchain*. A la hora de analizar su funcionamiento, tomaremos como ejemplo el *bitcoin*, pues se trata de la cadena de bloques más conocida y utilizada actualmente.

Para empezar, es necesario explicar la importancia de las claves públicas y privadas. Para realizar una transacción, la cadena *bitcoin* dispone de un fragmento secreto llamado clave privada, utilizada para firmar las operaciones. Así, proporciona una prueba matemática de que la transacción ha sido realizada por el propietario de estas criptomonedas. La firma también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Esta clave es un número de 256-bits que puede ser representado de muchas formas, por ejemplo, un número hexadecimal de 32 bytes o 64 caracteres en el rango de 0-9 o A-F.

Por cada clave privada que existe, se crea una clave pública por medio de un algoritmo unidireccional llamado ECDSA (Elliptic Curve Digital Signature Algorithm). Este algoritmo devuelve el mismo resultado siempre con el mismo input, pero no se puede invertir el proceso para obtener el input sabiendo el output (es decir, no se puede obtener una clave privada a partir de una pública).

Esta clave pública puede ser compartida con cualquier persona, ya que solo sirve a manera de identificación para recibir fondos en nuestra cuenta. La clave pública también es conocida como dirección. Este es un identificador de entre 27 y 34 caracteres alfanuméricos que empiezan con el número 1 o 3.

Las direcciones son de único uso, es decir, por cada transacción se debe generar una nueva clave pública asociada a la clave privada que va a recibir el dinero. Por otro lado, clave privada hay una sola y no es posible cambiarla o recuperarla si se olvida o pierde. Si se perdiese la clave privada, todos los *bitcoin* allí almacenados se perderán para siempre.

Ahora que entendemos (un poco) qué son las claves públicas y privadas, podríamos preguntarnos ¿qué pasaría si alguien adivina mi clave privada? La respuesta es que adivinar una clave privada es muy, muy improbable. El espacio total de direcciones de *bitcoin* ‘es de 2^{160}, un número difícil de imaginar, así que pensemos lo siguiente: en la Tierra hay aproximadamente 2^{63} granos de arena (incluyendo la arena que está en el fondo del océano). Ahora, imaginemos que por cada grano de arena creamos otro planeta Tierra y contamos todos los granos de arena de todos estos planetas. Tendríamos 2^{126} granos de arena, estando aún muy lejos del número mencionado anteriormente. Las claves públicas y privadas son por lo tanto unas herramientas muy importantes en el campo de la criptografía, y fundamentales para la seguridad de la *blockchain*.

Para seguir descubriendo más a fondo cómo funciona la criptografía dentro de las *blockchain*, hablaremos de la minería. La minería es el proceso de verificar transacciones realizadas e incluirlas dentro del libro mayor (cadena de bloques) del *bitcoin*. Este proceso está diseñado intencionalmente de manera que los nodos (ordena-

dores) encargados de confirmar las transacciones necesiten invertir un gran número de recursos. La dificultad de este trabajo es tal que el número de transacciones que pueden ser verificadas en un día es constante.

Cada bloque de transacciones tiene un sello conocido como *proof of work* (prueba de trabajo). Este sello es verificado por todos los otros nodos cada vez que se añade un bloque a la cadena. El *proof of work* es una pieza de información que es muy difícil de producir, pero muy fácil de verificar por otros. El trabajo de producir este sello es realizado por medio de un proceso aleatorio de prueba y error en el que hay muy poca probabilidad de acertar. La dificultad de este trabajo está ajustada para que se produzca un nuevo bloque aproximadamente cada 10 minutos, siendo este el tiempo que tardaría una transacción en ser procesada.

La minería necesita tener una recompensa, de lo contrario no se invertirían tantos recursos en esta especie de lotería criptográfica. Cuando un nuevo bloque es verificado, el minador recibe una recompensa en *bitcoin*. Actualmente, esta recompensa es de 12.5

BTC, aunque este valor es partido a la mitad cada 210,000 bloques. De esta forma, la cantidad total de *Bitcoin* está limitada a un máximo de 21 millones.

Morfología de los bloques

Los bloques son estructuras de datos que están diseñados para agrupar las transacciones y distribuirlas a todos los nodos de la red. Los bloques son creados por los mineros resolviendo el acertijo criptográfico que discutimos anteriormente (*proof of work)*.

Cada bloque está formado por un encabezado y el listado de transacciones. El encabezado es metadata (datos que describen un grupo de datos) que ayuda a verificar la validez del bloque. Éste incluye:

- la versión, que es el número o nombre de bloque;

- el *proof of work* del bloque anterior;

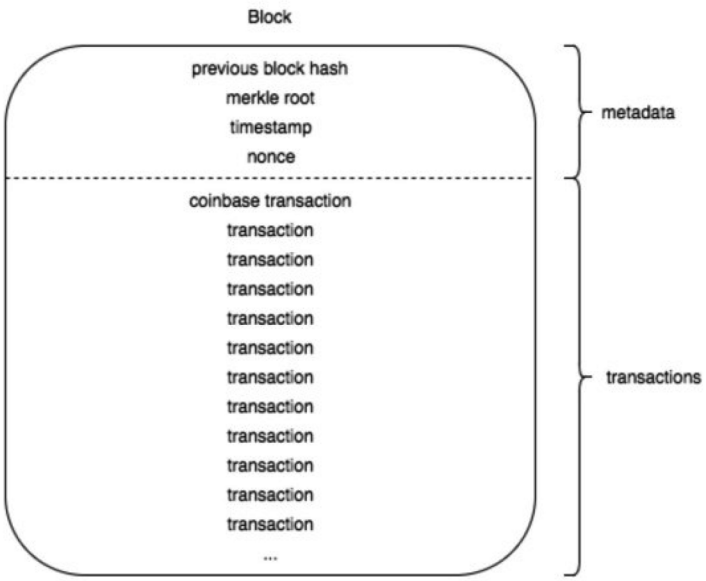
- la raíz de Merkle, código que el minero encuentra para validar el bloque y todas las transacciones de éste;

- la fecha y hora en la que el bloque fue creado;

- nBits, dificultad de encontrar el *proof of work* y crear el bloque; y

- nonce (number used once), valor aleatorio que el creador del bloque puede manipular como quiera.

Luego encontraremos el listado de transacciones que el minero ha decidido incluir en este bloque. Cada una de estas transacciones está validada, como vimos anteriormente, con el sistema de claves públicas y privadas. Al final de esta lista de transacciones, el minero incluye una extra en la que se otorga a sí mismo la recompensa por haber creado el bloque. Estos *Bitcoin* no pertenecen a nadie, son creados específicamente para recompensar a los mineros.



¿Qué utilidad tiene?

Hoy en día disponemos aún 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, vemos conveniente mostrar la infinitud de posibilidades que podría aportar a los diferentes sectores, no solamente económicos, sino también laborales, sociales e incluso militares como sucedió con internet.

El presente

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 gran cantidad de inversiones. Por lo tanto, la eliminación de estos intermediarios y sus costes asociados provocaría una mayor

disposición del público a la inversión, al tratarse de un sistema que conecta directamente al comprador y al 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.

El futuro

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.

En lo que concierne al sector de guardado o registro de datos, esta tecnología permite almacenar datos y archivos en una red Peer to peer (P2P); lo que permite 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 los datos compartidos. Esta verificación sería imprescindible en la entrega de curriculums por parte de los aplicantes a un trabajo, así como en el sector de la notaría, al poder verificarse la autenticidad de cualquier documento que haya sido previamente registrado en ella, eliminando así la necesidad de un fedatario público que tenga que certificarla.

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, de forma 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, a la vez 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.

Podemos concluir que esta nueva estructura informática tiene mucho que aportar a la sociedad. Sin embargo, podría acarrear la pérdida de trabajo en varios sectores. Por eso creemos que es de vital importancia la separación entre las ventajas y desventajas de la implantación de dicho sistema.

Implicaciones positivas.

Confidencialidad y anonimato

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.

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 del *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 ellos 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 financieras 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 el *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 por 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".

Anonimato

Uno de los mayores problemas de la *blockchain* procede precisamente de uno de sus "puntos fuertes": el anonimato. Sí 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 *bitcoin*s 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 ofrece 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, 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 Qatar afirmaba haber podido averiguar 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.

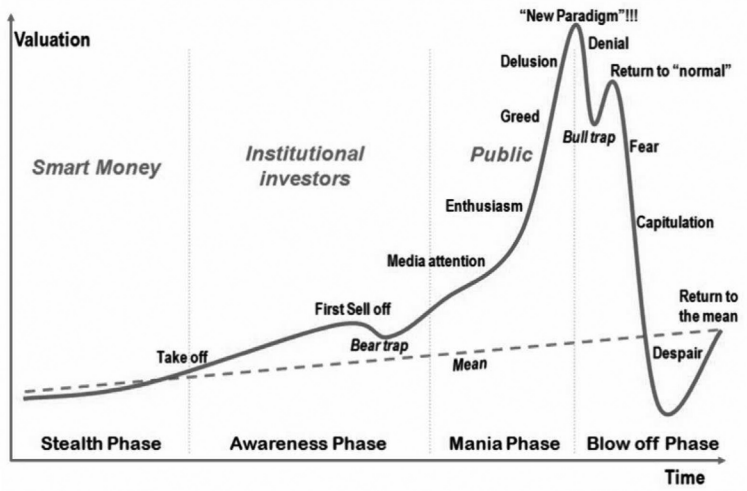
Seguridad

Otro de los pilares sobre los que se asienta la *blockchain* es la supuesta seguridad que ofrece esta tecnología. Sí es cierto que las cadenas de valores son de las tecnologías más seguras en la actualidad, pero 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 mucho 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.

La burbuja

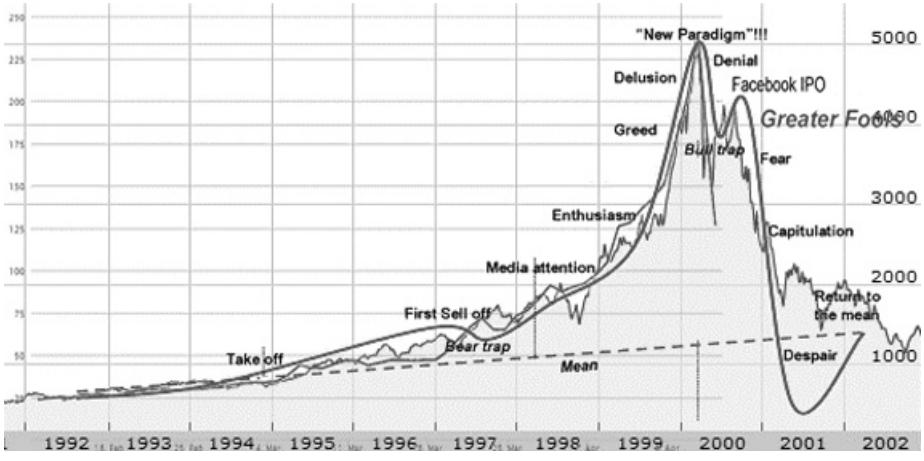
Otro tema preocupante, especialmente tras lo visto en los últimos dos meses, es la similitud entre la situación actual de las *blockchain*, especialmente en lo relacionado con las criptomonedas o monedas virtuales (y muy particularmente las *Bitcoin*) y la burbuja de las *dotcom* producida a finales de los años 90 y principios de los

2000. Para mostrarlo de manera visual vamos a estudiar este fenómeno con una serie de gráficas.

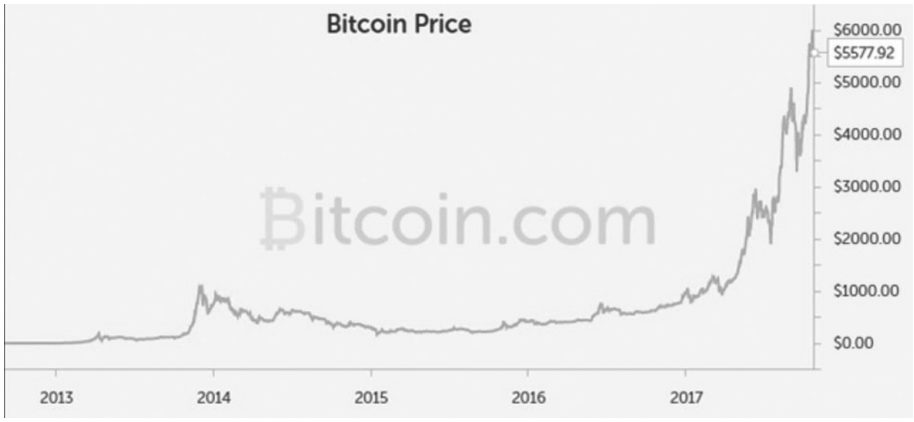


Fuente: Rodrigue, J. P. (2008)

Observemos ahora el parecido con la Burbuja de las *dotcom* de finales de siglo pasado:



Si ahora lo comparamos con el crecimiento del precio del *bitcoin*, el parecido es asombroso.



Fuente: *Bitcoin*.com (2010)

La primera es el modelo de burbuja económica propuesto por el profesor Jean Paul Rodrigue en 2008. Este modelo fue creado a partir del estudio de diferentes burbujas a lo largo de la historia, entre ellas, la Crisis de los tulipanes en los Países Bajos del siglo XVII, el Crash del 29, la Burbuja de las *dotcom*, la Crisis de las hipotecas subprime en 2007-2008...

¿A qué se debe esta burbuja? Las razones no están claras del todo, pero podríamos decir que la causa principal de esta impresionante subida y posterior bajada 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 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 gracias a esta burbuja, que se encuentra en sus instantes iniciales.

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 libre es necesario, sin embargo, que se den ciertos cambios.

Como hemos venido argumentando a lo largo de estas líneas, el impacto que está produciendo este nuevo modelo económico y social 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. Una de las principales diferencias entre la *blockchain* y el mercado actual es la descentralización y la confidencialidad que, llevadas al extremo, se pueden prestar a problemas legales y morales.

En el mercado del internet actual, existen ciertos entes 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 infinitud de transacciones que se pueden dar en el mercado.

Donde existen intercambios, rigen los principios de la Justicia Conmutativa, al venderse los diferentes productos al precio que cada uno considera "adecuado". Rige 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 al 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, en un futuro 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. De esta manera, comenzarán 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 del mercado, y gracias a la 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 a lo largo de la historia de la economía, y podemos afirmar que, quizás en unos años, estaremos hablando del fin de la *blockchain* y el comienzo de una nueva tecnología. Un nuevo sistema innovador y mucho más eficaz que pueda resolver de manera eficiente los problemas a los que se enfrentará la sociedad del futuro.

Bibliografía

Al Jawaheri, Husam; Al Sabah, Mashael; Boshmaf, Yazan y Erbad, Aimen (2018), "Cuando una pequeña filtración hunde un gran barco: desanonimizando usuarios de servicios secretos de Tor mediante el análisis de transacciones de *bitcoin*s", (Universidad de Qatar).

Collins, Aengus (2017), "Four Reasons to Question the Hype around *Blockchain*", publicado el 10 de julio de 2017, en www.weforum.org.

Lage, Óscar (2017), "Análisis de la ciberseguridad, ¿*blockchain* es realmente seguro?", en http://blogs.tecnalia.com/inspiring-blog/2017/11/30/analisis-la-ciberseguridad-*blockchain*-realmente-seguro/

Nakamoto, Satoshi (2008), "*Bitcoin*: A Peer- to-Peer Electronic Cash System", publicado el 1 de noviembre de 2008, en www.*Bitcoin*.org.

Preukschat, Alexander (2017), "El internet del futuro es la *blockchain* del internet del valor", publicado el 12 de enero de 2017, en www.oroyfinanzas.com

Preukschat, Alexander (2017), "Los fundamentos de la tecnología *blockchain*", en Preukschat, Alexander (coord.), *Blockchain: La revolución industrial de internet*, Gestión 2000, Barcelona, pp. 23-30.

Spaemann, Robert (2005), *Ética: cuestiones fundamentales*, Eunsa/Astrolabio, Barañáin, pp. 60-76.

Vega, Guillermo (2017), "Tres motivos para dudar de las bondades del *blockchain*", publicado el 15 de julio de 2017, en www.retina.elpais.com

Mitre Abuhayar, Carlos Alonso-Allende, Jesús María Escauriaza, Javier Gonzalo, Ricardo Márquez, Francisco Javier Moreno, e Iñaki Vélaz.