AUTOR → **Ramón Jesús Millán**
Ingeniero de Telecomunicación | www.ramonmillan.com

Tecnología *Blockchain*

La cadena de bloques segura, inalterable, transparente… y disruptiva!

La tecnología *blockchain* está siendo clave en el desarrollo de Internet debido a la capacidad que ofrece de transmitir valor de forma segura sin necesidad de intermediarios, permitiendo que un sistema distribuido puro pueda reemplazar los sistemas tradicionales centralizados y, así, producir cambios en múltiples sectores como la banca, las comunicaciones o los servicios públicos.

La traducción al castellano de *blockchain*, término también conocido como DLT *(Distributed Ledger Technology)*, sería "cadena de bloques". En términos sencillos, el *blockchain* es un 'libro de contabilidad' público de datos digital *(ledger)*, compartido entre una red P2P distribuida de nodos (ordenadores u otros dispositivos ejecutando un mismo software) independientes, sin que sea necesaria una autoridad central o intermediarios que aporten confianza a las transacciones [1].

Así como hace unos años, la tecnología P2P (Peer to Peer) era asociada con la piratería e intercambio de archivos ilícitos [2], en sus inicios el *blockchain* lo estaba con las monedas virtuales [3]. Esto ha generado una mala reputación, que ha dañado su credibilidad y confianza, relacionándola con el blanqueo de capitales, el fraude fiscal, el comercio de drogas, la especulación, la estafa, los crackers, Corea del Norte y Venezuela, etc.

Sin embargo, durante los últimos años la imagen del *blockchain* ha ido mejorando, pues aunque las criptomonedas han sido su primer uso práctico (Bitcoin, Dash, Ethereum, Litecoin, Monero, Ripple, Zcash, etc.), en realidad sus aplicaciones son múltiples. Sin lugar a dudas, el *blockchain* va a ser una tecnología clave y disruptiva en la evolución de Internet debido a su capacidad de conservar y transmitir valor de forma segura sin necesidad de intermediarios.

El *blockchain* va a ser una tecnología clave y disruptiva en la evolución de Internet debido a su capacidad de conservar y transmitir valor de forma segura sin necesidad de intermediarios

Bitcoin: la primera implementación de *blockchain*

Según cuenta la leyenda de Satoshi Nakamoto, el misterioso creador de Bitcoin, de quien aún no se ha conocido su identidad real, la revolucionaria criptomoneda, entró en funcionamiento en el año 2009 como un sistema de pagos P2P descentralizado y una moneda completamente digital, permitiendo así acabar con el oligopolio del sistema financiero mundial [4].

Bitcoin es una red distribuida de cadena de bloques pública basada en código abierto. Desde la perspectiva del usuario, Bitcoin no es más que una aplicación software, que provee un monedero personal y permite al usuario enviar y recibir *bitcoins* (moneda digital) con él. Bitcoin se compone de usuarios con carteras conteniendo claves, transacciones que se propagan a través de la red y mineros que producen -a través de cálculo computacional simultáneo y distribuido- el consenso de la cadena de bloques, que es el libro contable de todas las transacciones [3]. Esta contabilidad, puesto que contiene cada transacción procesada, permite verificar la validez de cada una de ellas.

La autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío. En Bitcoin cualquiera puede ayudar a procesar una transacción usando sus ordenadores y conseguir por ello una recompensa en *bitcoins*, lo cual se conoce comúnmente como minería *(mining)*. Sin embargo, conseguir convertirse en el ganador, al resolver los cálculos matemáticos o la “prueba de trabajo” *(proof of work)*, es cada vez más complicado: en la actualidad, ya casi es exclusivo de granjas de ordenadores ubicadas en países con bajo coste energético.

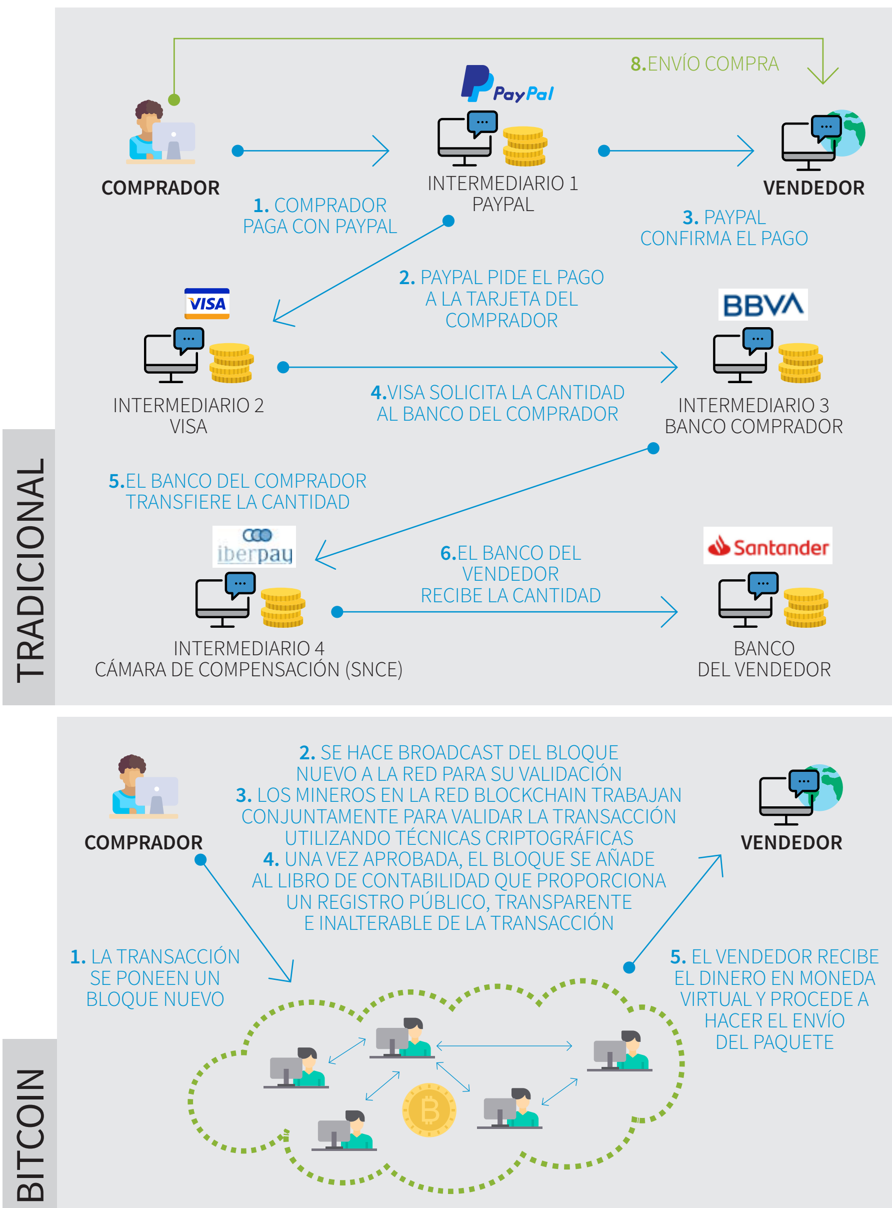
De este modo, para que las nuevas transacciones sean confirmadas, es necesario que se incluyan en un bloque con una prueba de trabajo matemático, proceso que tarda normalmente unos 10 minutos, pudiendo variar dependiendo de la capacidad de cálculo de la red. El bloque con las nuevas transacciones es verificado por los otros mineros y, si hay consenso, se almacena secuencialmente en la cadena de bloques principal, justo después del bloque de transferencias anterior.

En dos de las figuras adjuntas, se muestra una transacción de compra venta online utilizando la tecnología de pagos actual y la misma transacción, reduciendo el número de intermediarios, utilizando Bitcoin.

Funcionamiento del *blockchain*

En el año 2015 se puso en servicio Ethereum, una plataforma de código abierto descentralizada que permite la creación de contratos inteligentes entre pares, utilizando *blockchain*. Con ella se empezó a hablar de un *blockchain* 2.0, que facilita el intercambio de valor más allá de las monedas virtuales y expande el uso de *blockchain* a una gran variedad de aplicaciones gracias a los contratos inteligentes.

Sistemas de pagos **tradicional y Bitcoin**



Un concepto importante en este nuevo paradigma es el de token [6], que puede ser un bitcoin u otra moneda virtual, o bien un contrato inteligente, representando cualquier tipo de activo o utilidad (moneda, póliza de seguros, títulos de propiedad, votos, hipotecas, herencias, etc.) y pudiendo ser utilizado como prueba de propiedad, licencia software, certificados de acciones, un sistema de votación, un programa de fidelidad, etc.

El *token* está encriptado y, al irse almacenando, conforma la cadena de bloques. Más específicamente, un contrato inteligente *(smart contract)* es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones programadas con anterioridad sucedan automáticamente, como resultado de que se cumplan una serie de condiciones o cláusulas específicas [5]. Es decir, son contratos que se ejecutan y cumplen de manera automática y segura, reduciendo el fraude, los costes y la burocracia.

El *blockchain* utiliza un sistema criptográfico de clave pública *(public key)*, también conocido como de clave asimétrica *(asymmetric)*. Cada cuenta (o dirección) de *blockchain* tiene dos claves, una pública y otra privada [1]. La clave privada es la que tiene la información sobre el usuario, garantizando su identidad y su anonimato, permitiéndole acceder a sus activos. Esta clave no debe ser compartida con otras personas y, si se pierde, los activos asociados también. En general, un mensaje cifrado con la clave privada de un usuario y sólo podrá descifrarse con la clave pública de ese mismo usuario, asegurando que fue esa persona, propietaria de esas claves, quien envió ese mensaje. Por otro lado, si un mensaje se cifra con la clave pública de un usuario, sólo ese usuario podrá descifrar el mensaje con su clave privada. Cualquier transacción funciona de forma parecida.

Los bloques que se almacenan digitalmente en *blockchain*, mezclan la información de las direcciones de las partes involucradas en la transacción, la cantidad de unidades de valor o tokens en movimiento y una marca temporal. Luego, las procesa a través de una función llamada hash [5]. Esta función hash es un complejo algoritmo criptográfico que condensa en una secuencia alfanumérica única de longitud fija, información de cualquier extensión.

Esta información es la huella dactilar *(fingerprint)* o hash del bloque y es imposible encontrar dos entradas en el *blockchain* con el mismo valor. El problema es lo que todos los nodos de la red tratan de resolver con el fin de confirmar lo que contiene la transacción y enlazarla al bloque previo. Puesto que cada bloque tiene un *hash* enlazando al bloque previo, la información en el *blockchain* es fácilmente verificable e imposible de eliminar.

Ventajas del *blockchain*

Blockhain ha suscitado un gran interés porque permite que un sistema distribuido puro tenga el potencial de reemplazar los sistemas tradicionales centralizados y revolucionar múltiples industrias debido a la desintermediación. Al trabajar sobre una base de datos distribuida, los distintos usuarios de esa red hacen la labor tradicional del intermediario, ya que almacenan una copia de cada transacción en forma de bloques. En primer lugar, esto dota a *blockchain* de una alta redundancia.

Además, *blockchain* es una de las tecnologías más seguras que existen [8], al menos hasta la futura llegada de los ordenadores cuánticos. Puesto que los datos están encriptados en una base de datos distribuida y entrelazada y se necesita el acuerdo unánime de todos los nodos para que la transacción sea validada, las posibilidades de atacar una red *blockchain* y tener éxito son muy bajas, ya que la capacidad de computación necesaria para comprometerla sería muy elevada.

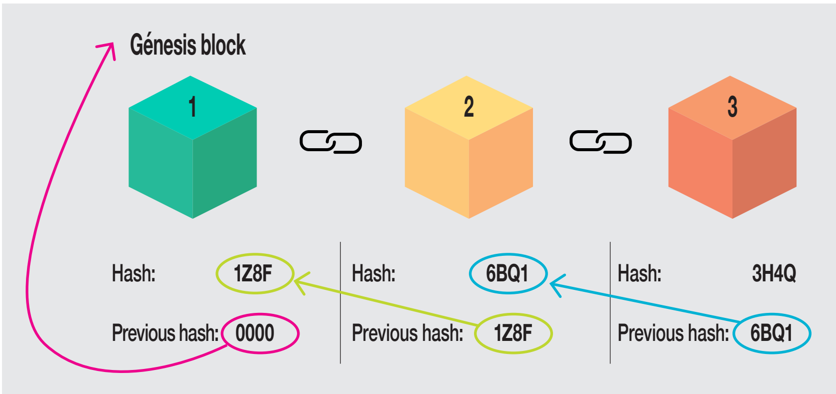
Por otro lado, una vez introducida la información en el *blockchain* no puede ser borrada o modificada, solo se podrán añadir nuevos registros y no serán legitimados a menos que la mayoría de los nodos se pongan de acuerdo para hacerlo. Es decir, otra característica muy interesante del *blockchain* es la inalterabilidad, trazabilidad y transparencia; que permite ofrecer una visión única sincronizada de la información, agilizando y automatizando el proceso de verificación de la información y eliminando errores humanos [1].

Algunas limitaciones

Sin embargo, cabe destacar que los protocolos utilizados para validar transacciones en el *blockchain* requieren de un tiempo variable y relativamente extenso para ser completado, que va de minutos a horas, dependiendo de los picos de carga. Es decir, en el caso de aplicaciones que requieran una baja

Guía rápida para no perderse con el *blockchain*

- **TECNOLOGÍA P2P**: del inglés peer to peer (entre pares). Red descentralizada sin clientes ni servidores fijos, que cuenta con una serie de nodos que funcionan simultáneamente como clientes y servidores de los demás nodos de la red, cada uno de los cuales puede iniciar, detener o completar una transacción compatible.
- **CRIPTOMONEDA**: también llamada criptodivisa, es un tipo de divisa alternativa o moneda digital, que utiliza criptografía fuerte para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos.
- ***LEDGER* (LIBRO DE CONTABILIDAD)**: fichero físico o digital donde se registran todas las transacciones realizadas por los usuarios de una entidad o empresa. En Bitcoin, lugar público donde están registradas todas las operaciones que se han realizado desde el inicio del proyecto.
- ***TOKEN***: unidad de valor emitida por una entidad privada, con usos más amplios que Bitcoin ya que puede representar cualquier activo o utilidad y ser utilizado como prueba de propiedad, licencia software, certificados de acciones, un sistema de votación, un programa de fidelidad…
- ***SMART CONTRACT* (CONTRATO INTELIGENTE)** : programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones programadas con anterioridad sucedan automáticamente, si se cumplen una serie de condiciones.
- ***MINING* (MINERÍA)**: en Bitcoin, proceso de creación o descubrimiento de bitcoins, a través de transacciones matemáticas, que quedarán registradas en el *ledger.*
- ***PROOF OF WORK* (PRUEBA DE TRABAJO)**: cálculos matemáticos que integran el proceso de *mining*.
- **ETHEREUM**: plataforma de código abierto, descentralizada, que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo *blockchain.*
- ***PUBLIC KEY* (CLAVE PÚBLICA)**: componente del método criptográfico de clave pública *(public key cryptography)*, en la que cada usuario tiene un par de claves, una privada y otra pública. La clave pública se puede entregar a cualquier persona, mientras que la otra, la clave privada, ha de ser guardada por el propietario. Si un mensaje se cifra con la clave pública de un usuario, sólo ese usuario podrá descifrar el mensaje con su clave privada. Un mensaje cifrado con la clave privada podrá descifrarse con la clave pública, asegurando que fue el usuario propietario de esas claves quien envió ese mensaje.
- ***HASH***: algoritmo criptográfico que condensa en una única cadena de letras y números, con una longitud fija, información de cualquier extensión, incrementando su seguridad. A través de él se procesa la cantidad de unidades de valor o *tokens*.
- ***FINGERPRINT***: información resultante de la función hash.



Fragmento del vídeo "How Does a Blockchain Work – Simply" [7].

latencia, son generalmente mejores los sistemas centralizados.

Por otro lado, si es necesario intercambiar mucha información en las transacciones, *blockchain* es también una solución más costosa respecto a los sistemas centralizados, puesto que los datos tienen que ser replicados y validados por múltiples nodos de la red, aumentado las necesidades de almacenamiento y procesamiento, así como el consumo energético.

En múltiples sectores

El boom mediático de los últimos años ha creado la falsa percepción de que el *blockchain* va a terminar por completo con todos los sistemas centralizados y con los intermediarios tradicionales –bancos, emisores de medios de pago, notarios, etc.–. Sin embargo, ambos sistemas se complementarán, ya que como hemos visto, también hay limitaciones técnicas inherentes al *blockchain*. También es necesaria la adaptación del complejo marco regulatorio que realmente será específico a cada caso de uso, industria y país donde se aplique. Con el tiempo, será necesaria la interoperabilidad entre distintos tipos de *blockchain.*

El *blockchain* tendrá un importante papel en las transferencias de dinero internacionales, reduciendo sensiblemente los intermediarios involucrados y sus comisiones. También tendrá un rol destacado en el mercado de capitales e inversión (acciones, bonos, derivados, etc.), productos de crédito, productos de ahorro, contabilidad y auditoría de transacciones financieras, etc.

Los bancos, aseguradoras, notarías, etc., podrían trabajar con contratos inteligentes, personalizándolos más al perfil concreto de cliente, agilizando los trámites y reduciendo sus costes. Por ejemplo, si se detecta el fallecimiento de una persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos, e incluso se podría llegar a automatizar el cambio de propiedad en el registro y el pago de impuestos.

El sector público también puede beneficiarse mucho del *blockchain*, permitiendo una importante reducción de costes y un mejor servicio a ciudadanos y empresas. Entre las aplicaciones está el registro de títulos de la propiedad, el control de subvenciones, el voto electrónico, los registros sanitarios, la gestión de licencias, etc.

El *blockchain* puede aportar mejoras a la industria del entretenimiento y medios, por ejemplo, pueden lanzar servicios para manejar más eficientemente las licencias y los pagos de royalties o mejorar las medidas de audiencia y detectar y combatir el fraude. En las industrias que tienen procesos de fabricación y distribución, hay beneficios por la mejora de la transparencia en toda la cadena de suministro, gestionando mejor la información relacionada con el origen del producto, precio y ubicación, además de la gestión logística y del transporte. Estas mejoras ayudarán a optimizar las cantidades de unidades y su disponibilidad en tiendas.

También es una tecnología muy prometedora para luchar contra la falsificación de productos y marcas. El *blockchain* puede también jugar un rol importante en el sector de las telecomunicaciones, en aspectos como la detección de fraude, la gestión de identidad, la autenticación y gestión de la seguridad en IoT, etc. ■

Esta tecnología permite que un sistema distribuido puro tenga el potencial de reemplazar los sistemas tradicionales centralizados y revolucionar así múltiples industrias debido a la desintermediación

Bibliografía

[1] 'Blockchain Basics. A Non-Technical Introduction in 25 Steps'. Daniel Drescher. Apress, 2017.
[2] 'Domine las redes P2P *(Peer To Peer)*'. Ramón Jesús Millán Tejedor. Creaciones Copyright, 2006.
[3] 'Mastering Bitcoin: Unlocking Digital Cryptocurrencies'. Andreas M. Antonopoulos. O'Reilly, segunda edición, 2017.
[4] 'Monetary policy in the digital age'. Crypto assets may one day reduce demand for central bank money. Dong He, Finance & Development, Junio 2018.
[5] 'Blockchain for dummies'. Tiana Laurence, John Wiley & Sons, 2017.
[6] 'OECD Blockchain Primer'. OCDE (Organización para la Cooperación y el Desarrollo Económicos), 2018.
[7] 'How Does a Blockchain Work – Simply'. Xavier Savjee, YouTube, 2017.
[8] 'Exploración de las tecnologías blockchain desde el punto de vista de la ciberseguridad y privacidad'. Javier Areitio Bertolín. Conectrónica, nº 212, GM2 Publicaciones Técnicas, 2018.