Blockchain

Un poco de Historia.

El sistema blockchain, aparecido en el 2009 junto con la moneda virtual bitcoin, es un registro de las transacciones digitales que se basa en una gigantesca base de datos en la que están inscritas todas las operaciones financieras realizadas con la divisa electrónica.

Que es Blockchain

Lo primero es contextualizarlo. **Blockchain significa "cadena de bloques"**, su propio nombre nos será muy ilustrativo más adelante para comprender cómo funciona. Nació como actor secundario en la revolución del **bitcoin**, ya que se trata **de la tecnología o el sistema de codificación de la información que está por detrás de la moneda virtual** y que sustenta toda su estructura. Pronto se vio el potencial que tenía por sí misma y **la cantidad de aplicaciones que permite en otras áreas más allá de las transacciones financieras**, como la administración pública o el Internet de las cosas.

Blockchain es una tecnología que permite **la transferencia de datos digitales con una codificación muy sofisticada y de una manera completamente segura**. Sería como el libro de asientos de contabilidad de una empresa en donde se registran todas las entradas y salidas de dinero; en este caso hablamos de un **libro de acontecimientos digitales**. Pero además, contribuye con una tremenda novedad: **esta transferencia no requiere de un intermediario centralizado que identifique y certifique la información, sino que está distribuida** en múltiples nodos independientes entre sí que la registran y la validan sin necesidad de que haya confianza entre ellos. Una vez introducida, **la información no puede ser borrada**, solo se podrán añadir nuevos registros, y no será legitimada a menos que la mayoría de ellos se pongan de acuerdo para hacerlo.

Junto al nivel de seguridad que proporciona este sistema frente a hackeos, encontramos otra enorme ventaja: **aunque la red se cayera, con que solo uno de esos ordenadores o nodos no lo hiciera, la información nunca se perdería** o el servicio, según el caso del que hablemos, seguiría funcionando. Un ejemplo que ilustra la importancia de la red distribuida está en las redes sociales. Con este sistema, **blockchain eliminaría la centralización que imponen aplicaciones como Facebook o Twitter** a la hora de identificarnos o validar la procedencia de nuestros mensajes, y la integridad de los mismos sería garantizada por la red de nodos.

Quién es quién en el blockchain y cómo funciona

Vamos a intentar descifrar quién participa en el blockchain y cómo funciona su tecnología. El blockchain, como su nombre indica, es **una cadena de bloques**. Cada uno de esos bloques contiene la información codificada de una transacción en la red. Antes hicimos la analogía del libro contable, donde anotamos, por ejemplo, que salió A y entró B. Pues bien, blockchain se comporta igual, pero será la red de nodos distribuidos quienes tengan que certificar que esos datos son verdaderos ¿Cómo lo hacen? Cada **bloque de la cadena** porta el **paquete de transacciones y dos códigos**, uno que indica cuál es el bloque que lo precede (excepto el bloque origen, claro), y otro para el bloque que le sigue, es decir, que están entrelazados o encadenados por lo que se llaman códigos o apuntadores **hash**. Ahora entra en juego el concepto de **minado** que realizan los **nodos**, es decir, el proceso de validación de la información. En este proceso de minado o comprobación, cuando hay dos bloques que apuntan al mismo bloque previo, sencillamente gana el primero en ser desencriptado por la mayoría de los nodos, es decir, que **la mayoría de puntos de la red deben ponerse de acuerdo para validar la información**. Por eso, aunque blockchain genera múltiples cadenas de bloques, siempre será legitimada la cadena de bloques más larga.

Cuál es el futuro del blockchain

Los expertos comparan la llegada del blockchain con hitos como la integración de los

ordenadores en el uso doméstico o el desarrollo de Internet, es decir, **un sistema que cambiará nuestra forma de entender los negocios y la sociedad.**

Uno de sus mayores potenciales está en los llamados **smart contract** o contratos inteligentes, es decir, con la tecnología del blockchain se podrán hacer acuerdos y transacciones de forma confiada sin revelar información confidencial entre las dos partes y sin la necesidad de "**árbitros**", como **pagos a distribuidores** o, por ejemplo, **el alquiler de un coche de forma online.**

Pero no solo esto, basado en el mismo concepto, **blockchain será esencial para el Internet de las cosas.** Nuestros aparatos electrónicos podrán comunicarse entre sí de forma segura y transparente, y pronto veremos a nuestro frigorífico comprándonos yogures en el supermercado online en cuanto detecte que se han terminado.

La administración tendrá una baza incomparable con este sistema de criptografía. Cuestiones como la del **voto electrónico** que, a pesar de los intentos realizados con otras tecnologías, no ha resistido a los hackeos, ahora podría ser una opción viable para los votantes con la seguridad de que su identidad no será suplantada y la comodidad de no tener que desplazarse hasta el colegio electoral. Actualmente son muchos los proyectos en los que se está investigando para implantar el blockchain como estructura que los respalden, así que pronto veremos si realmente se convierte en la tecnología del futuro.

Tipos Blockchain y funcionamiento

Hay muchas cadenas de bloques. Tantas como queramos. Pueden estar interconectadas entre sí. Y pueden usarse para muchas cosas distintas. Para cualquier transacción, en realidad. Las hay de dos tipos: públicas y privadas (bueno, en realidad también las hay híbridas). Las públicas son, por ejemplo, sobre las que trabajan bitcoin (que fue la primera blockchain que hubo) o ethereum. Aquí puede entrar quien quiera. En las privadas solo pueden entrar quienes digan los propietarios. Y tienen usos concretos.

Recordemos: una blockchain es una inmensa base de datos que se distribuye entre varios participantes. Es decir, es un libro de registro (ledger en inglés) inmutable que contiene la historia completa de todas las transacciones que se han ejecutado en la red. A cada participante se le llama nodo, que en realidad viene a ser un ordenador más o menos potente. Estos nodos se conectan en una red descentralizada, sin un ordenador principal. Son redes llamadas P2P que hablan entre sí usando el mismo lenguaje (protocolo).

Al mensaje que transmiten se le llama token. Un token (en inglés significa símbolo, señal o ficha) no es más que una representación de la información que aloja la red. Esta información puede representar cualquier tipo de activo, bien o servicio, como por ejemplo dinero en forma de bitcoins, un alquiler de un chalet o una compra de energía. Lo que se quiera (siempre que lo permita la ley). La información viaja encriptada, gracias a lo cual puede estar distribuida sin que se revele su contenido.

Las transferencias de tokens se agrupan en bloques que se van generando cada cierto tiempo. Las nuevas transferencias que no han cabido en un bloque se han de agrupar en el siguiente, el cual va indisolublemente enlazado al anterior. Y así sucesivamente. De ahí el nombre cadena de bloques.

Aplicaciones de la tecnología blockchain

Como parte del sistema Bitcoin, su funcionalidad es básicamente la de proporcionar un **registro o libro de contabilidad distribuido** en el que se van almacenando las diferentes transacciones realizadas con bitcoins. Cada 10 minutos aproximadamente se genera un bloque con la información de las transacciones que se han realizado durante ese período de tiempo. El bloque es verificado por los propios miembros de la comunidad Bitcoin y, si hay **consenso**, se almacena en la *blockchain* o cadena de bloques principal, justo a continuación del bloque de transferencias anterior.

Esta cadena de bloques **es pública** y puede ser consultada en cualquier momento por cualquiera; además, **no existe una copia única** de la cadena, sino que se trata de un sistema descentralizado en el que **cada nodo almacena una copia**.

De ese modo no solo desaparecen los intermediarios, disminuyendo el coste de las transacciones, sino que **el sistema es mucho más seguro, transparente e inalterable**. Además, la tecnología blockchain tiene otra peculiaridad y es que cada usuario tiene una clave criptográfica privada asociada a otra clave pública. La clave privada es la que contiene toda la información sobre el usuario y garantiza su identidad, mientras que la clave pública solo muestra lo que el usuario desea que los demás puedan ver.

Para enviar dinero, el usuario necesita acreditar que tiene en su poder la clave privada para demostrar que es quien dice ser y firmar con ella la transacción, mientras que para recibir dinero basta con proporcionar la clave pública.

Eso **proporciona cierto anonimato en las transacciones,** algo que ha sido muy criticado en el sistema Bitcoin, por facilitar las transacciones de negocios turbios.

Aplicaciones de la tecnología blockchain dentro del sistema financiero

Sus aplicaciones dentro del sistema financiero más allá de Bitcoin son muchas, de ahí que haya despertado tanto interés entre los bancos y otras entidades financieras.

Según el Foro Económico Mundial, en los próximos años seremos testigos de una importante transformación en la que la blockchain acabará convirtiéndose en el “corazón” del futuro sistema financiero mundial.

Recientemente, el 80% de los bancos ha reconocido estar trabajando ya en el desarrollo de productos basados en esta tecnología y, según una encuesta realizada por IBM, el 15% de los bancos entrevistados indicó que sus servicios basados en blockchain empezarán a funcionar a escala comercial antes de que finalice 2017.

Entre sus aplicaciones están:

- La posibilidad de **agilizar los pagos y transferencias y el envío de remesas, abaratando considerablemente su coste:** por ejemplo, la startup estadounidense Abra está desarrollando un sistema digital global de gestión de activos, con funciones de banca minorista como pagos y

ahorros y basado en la blockchain de bitcoin que ya **permite, entre otras cosas, el envío prácticamente instantáneo de remesas** a otros países desde el móvil y por alrededor de un 0,25% del coste actual.

- **Mercados de valores:** por ejemplo, Nasdaq ya utiliza la tecnología blockchain en su mercado de valores privado, uno de los mayores del mundo.
- **Mercados de predicción descentralizados:** Augur es un mercado de predicción descentralizado que permite a sus usuarios comprar y vender acciones anticipándose a un suceso en base a la probabilidad de que se produzca uno u otro desenlace.

Sin embargo, las aplicaciones de la tecnología *blockchain* no se limitan al sistema financiero, si no que son mucho más variadas.