Equipo Fintech
16 de febrero de 2017

La tecnología Blockchain en el sistema Bitcoin

La tecnología *blockchain* se dio a conocer, por primera vez, como tecnología que sustenta el sistema de la famosa criptomoneda Bitcoin, creada por Satoshi Nakamoto.

Pero, ¿qué es en realidad la tecnología *blockchain* y por qué está despertando tanto interés últimamente?

La funcionalidad de la *blockchain* o cadena de bloques es básicamente la de proporcionar un **registro o libro mayor distribuido e inmutable** en el que se van almacenando las diferentes transacciones realizadas con bitcoins.

Al ser un sistema distribuido en red, es mucho más seguro, dado que no hay una sola copia del registro como en los sistemas centralizados, sino que cada nodo de la red almacena una copia.

De esta forma, **son los propios usuarios quienes tienen el control,** en lugar de un ente centralizado, ya sea un gobierno, entidad financiera, etc.

Por otro lado, la verificación e integridad de la información la garantizan los propios miembros de la red, por lo que **desaparecen los intermediarios** y se abaratan los costes.

Ya solo por esto, desde su creación ha despertado gran interés, pero además, poco a poco **han ido surgiendo otras *blockchains* con ligeras variaciones y nuevas aplicaciones**, no solo dentro del sistema financiero, sino también fuera de él.

Un claro **ejemplo** es la *blockchain* **Ethereum** que, entre otras novedades, incorpora la posibilidad de crear los denominados *smart contracts* o contratos inteligentes.

Los expertos comparan ya la tecnología *blockchain* con la creación de Internet y afirman que **lo revolucionará todo**, desde el sector financiero, al de la energía; e incluso el de la música.

Sin embargo, para poder entender sus enormes posibilidades de aplicación es necesario primero tener una idea de cómo funciona esta tecnología.

Cómo funciona el sistema Bitcoin

El sistema consta de un protocolo Bitcoin y una red P2P del mismo nombre, similar a las redes P2P de intercambio de archivos con múltiples nodos (ordenadores conectados a ella).

Las distintas fases del funcionamiento son las siguientes:

1. **Transacción.** Cuando cualquier usuario realiza una transacción en bitcoins, transmite esa información en forma de mensaje a la red.

2. **Retransmisión.** Los nodos cercanos captan esa información y verifican si la transacción es correcta. Si no es correcta, simplemente, la ignoran, pero si es correcta, la almacenan en su lista de transacciones pendientes de añadir a la *blockchain* y la retransmiten a todos los nodos cercanos.

   Estos, a su vez, la verificarán y, dado que es correcta, la almacenarán en su lista de transacciones pendientes y la comunican también a sus nodos cercanos; y así, se irá retransmitiendo una y otra vez para que llegue al mayor número posible de nodos en la red.

3. **Creación de bloques.** Cada 10 minutos, aproximadamente, generan un bloque con la información de las transacciones que han recibido durante ese tiempo.

   En la creación de cada bloque se genera también un ***hash***, una clave generada con técnicas criptográficas a partir de la información contenida en dicho bloque y que es única para cada bloque.

   Los bloques generados por los nodos pueden tener diferencias entre sí, dado que no todos reciben información de todas las transacciones realizadas, debido a problemas en las comunicaciones: paquetes perdidos, nodos caídos temporalmente por problemas en la red, etc.

4. **Minería.** ¿Cómo se elige entonces cuál será el siguiente bloque que se unirá a la cadena de bloques?

   Pues se utiliza un sistema denominado ***proof-of-work***, en el que los nodos compiten entre sí utilizando su potencia de computación.

   Para ello, deben resolver unos problemas matemáticos que se conocen como *hash puzzles* y que, básicamente, consisten en encontrar un número denominado ***nonce***, que encaje para la función *hash* de dicho bloque.

   La resolución de estos "puzzles" criptográficos requiere unos ordenadores extremadamente potentes y con gran capacidad de computación, por lo que solo los nodos con gran capacidad de computación, conocidos como **"mineros"**, se molestan en competir por resolverlos.

   Los mineros prueban con diferentes números hasta descubrir el *nonce* para ese bloque.

5. **Unión del bloque a la cadena.** El primer nodo minero en resolver el *puzzle* transmite su hallazgo a la red, incluyendo en el bloque enviado el hash del último bloque incorporado ya a la cadena de bloques.

   De este modo, el nuevo bloque queda enlazado a la cadena de bloques a través de los *hash*, aunque de forma provisional, hasta que haya consenso.

   Los demás nodos reciben el bloque y comprueban si es correcto, recalculando el *hash* y verificando que todas las transacciones que contiene sean correctas.

   Si no es correcto, simplemente lo ignoran y esperan al siguiente bloque para volver a realizar sus comprobaciones, pero si es correcto, lo almacenan en su copia de la blockchain y lo comunican a otros nodos para que también puedan comprobarlo y retransmitirlo a su vez.

   Si hay **"consenso" general** en que todo es correcto, es decir, se dan cada vez más

confirmaciones positivas, el bloque propuesto por el minero que ha resuelto el puzzle queda definitivamente añadido a la ***blockchain* o cadena de bloques**.

6. **Recompensa.** Como compensación por su trabajo, los mineros reciben **una cantidad de bitcoins de nueva creación**.

   Para cobrarlos, al generar el bloque, el minero añade una transacción de nueva creación de bitcoins y otra que transfiere esos bitcoins recién creados a su cuenta. Este es el **único modo de acuñar nuevos bitcoins**.

   No obstante, no pueden poner la cantidad que quieran, sino que hay una cantidad ya estipulada como recompensa por cada bloque resuelto. Actualmente, esta recompensa es de **12,5 bitcoins** (12.155,12€ al cambio actual - 16/02/2017).

Fuente: cotizacionbitcoins.com

   Es importante señalar que esta cantidad se reduce a la mitad cada cierto tiempo, mermando los beneficios de los mineros; y que tarde o temprano llegará a cero.

7. **Comisiones.** Los mineros también obtienen ingresos de las comisiones por transacción. Se trata de otra forma de recompensa, aunque mucho menos lucrativa que la anterior.

   Y es que, al igual que en las transferencias de dinero tradicionales, en las transferencias de bitcoins también puede haber comisiones. La diferencia, básicamente, es que en el sistema Bitcoin **son opcionales y completamente voluntarias**.

Es **el propio usuario**, en el momento de realizar una transacción de envío de dinero a otro usuario, el que **elige añadir o no una comisión** que irá a parar al minero que resuelva el bloque en el que incluya su transacción.

Pero… ¿Por qué pagar una comisión si podemos realizar el envío sin ella? Pues básicamente, porque los mineros, a la hora de decidir qué transacciones incluyen en el siguiente bloque propuesto, darán prioridad, dentro de lo posible, a aquellas que incluyen una comisión y que, por lo tanto, les van a reportar mayor beneficio.

Incluir una comisión en nuestra transacción ayudará a que acabe antes en la cadena de bloques.

Seguridad y transparencia

Por seguridad, cada bloque almacenado en la *blockchain* contiene su *hash* y el del bloque anterior. De este modo, **se garantiza que nadie pueda crear un bloque e insertarlo en la cadena**, dado que no coincidirían los *hash*.

Para intentar alterar una parte de la cadena y que nadie lo perciba sería necesario ir alterando uno a uno cada bloque hasta el origen, algo que requeriría una capacidad de computación descomunal y muchísimo tiempo.

Además, **la cadena de bloques es pública,** por lo que puede ser consultada en cualquier momento por cualquiera; y, no existe una copia única de la misma, sino que, como sistema descentralizado, **cada nodo almacena una copia** que se actualiza cada vez que se añade un bloque nuevo a la cadena.

Para evitar el problema del **"doble gasto"** y evitar que un usuario cometa el fraude de transferir más de una vez los mismos bitcoins en diferentes transacciones, la información de cada transacción incluye el *hash* del bloque que contiene la transacción en la que el usuario recibió esos bitcoins y que, por lo tanto, le acredita como su propietario.

De este modo, no solo desaparecen los intermediarios, disminuyendo el coste de las transacciones, sino que **el sistema es mucho más seguro, transparente e inalterable**.

Claves de usuario. Pseudoanonimato

La tecnología *blockchain* de Bitcoin tiene una peculiaridad que es el foco central de las críticas que recibe continuamente: **garantiza cierto anonimato en las transacciones** y, por tanto, puede ser utilizada en transacciones de negocios turbios, como narcotráfico o terrorismo.

Cada usuario tiene una clave criptográfica, que consta a su vez de una clave 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 el propietario de los bitcoins que se dispone a transferir, mientras que para recibir dinero basta con proporcionar la clave pública.

De este modo, aunque cualquiera puede tener acceso a la información almacenada en la cadena de bloques **no es posible ver los datos de las personas que realizan las transacciones**, **sino solo su clave pública**.

No obstante, el anonimato no está garantizado al 100%, puesto que la cadena de bloques es pública y, por lo tanto, rastreable.

Aunque no aparezcan los nombres de las personas que participan en cada transacción, sí aparecen sus claves públicas y es posible hacer un seguimiento, a lo largo de toda la cadena de bloques, del traspaso de cada bitcoin hasta su creación y conocer el saldo real de cada clave.

Para conocer el histórico de las operaciones de una persona, tan solo es necesario conseguir relacionar una clave pública con una identidad real, algo que no es tan difícil que suceda a la larga, si la persona utiliza una misma clave durante mucho tiempo.

Para dificultar este rastreo, muchos usuarios optan por utilizar más de una clave y cambiarlas con frecuencia.

Conclusión

Hasta la creación de la tecnología *blockchain* no era posible enviar dinero directamente entre usuarios. Había que recurrir siempre a algún intermediario o entidad central de control que validase la transacción.

Sin embargo, gracias a esta tecnología, en el sistema Bitcoin quedan completamente fuera de la ecuación.

Solo por esto ya constituye una innovación asombrosa de por sí, pero además, con el tiempo se ha puesto de manifiesto que es posible utilizar esta tecnología para registrar muchos otros tipos de información, además de las transacciones realizadas con bitcoins.

Dado que se trata de código abierto, cualquiera puede modificar su código para crear nuevas variantes adaptadas a diferentes usos; y eso es precisamente lo que ha sucedido en los últimos años, con la aparición de diferentes *blockchains*.

En este sentido, la tecnología *blockchain* ofrece la posibilidad de transformar gran parte de la sociedad como la conocemos actualmente, descentralizando prácticamente cualquier sector y abaratando los costes.

De ahí que lleguen a compararla con la aparición de internet.

Y es que su creación, parece haber marcado el principio de una transformación que afectará a la vida diaria de las personas y empresas en áreas muy diversas.

En poco tiempo lo sabremos.