Blockchain (características y funcionamiento)

Blockchain y computación cuántica

tech

CONTENIDO

Objetivos

- Conocer las principales características de blockchain.
- Aprender el funcionamiento de blockchain estudiando los pasos necesarios para la ejecución de una transacción.
- Profundizar en el funcionamiento de los principales elementos que componen la tecnología blockchain.

Principales características de *Blockchain*

La **tecnología *blockchain*** presenta una serie de características que permiten **gestionar la información de manera segura y trazable**, proporcionando **transparencia y privacidad** a los participantes.

Estas características resultan muy interesantes en el entorno empresarial y permiten a las empresas mejorar algunos de los procesos de negocio existentes y definir nuevos modelos de negocio basados en entornos colaborativos soportados por la tecnología *blockchain*.

En los siguientes apartados se exponen las principales características asociadas a la tecnología *blockchain*.

Seguridad

Tal y como se comentó en la introducción a *blockchain*, **la criptografía** es un elemento **esencial en la tecnología** *blockchain*, proporcionando seguridad sobre la información que se almacena en la cadena de bloques y la información compartida entre los nodos de la red.

Para poder operar en la red es necesario disponer de un conjunto de claves asimétricas válidas para operar en el *blockchain* correspondiente. No todos los *blockchain* usan el mismo formato de claves asimétricas.

En *blockchain* todas las transacciones van firmadas por la clave privada del emisor y dentro de la transacción se incluye la clave pública que permite verificar el contenido de la transacción, detectando si la transacción ha sido manipulada.

Las **funciones *hash*** son otro de los elementos **que proporcionan seguridad a la cadena de bloques**, ya que permiten generar identificadores únicos del contenido de los bloques. Estos identificadores de los bloques se utilizan para interconectar los bloques, ofreciendo un mecanismo que permite identificar alteraciones en la cadena.

Los bloques y transacciones son validados por toda la red de nodos, proporcionando seguridad sobre la información que se incorpora en *blockchain*.

La seguridad radica en la capacidad que tienen los nodos en detectar modificaciones de los datos rápidamente, rechazando la transacción o el bloque.

Trazabilidad

Esta es una de las características que desde la perspectiva de auditoría resulta muy interesante. ***Blockchain* permite recorrer la cadena de bloques** y trazar todas las operaciones que se han realizado sobre una determinada dirección; o retroceder en el tiempo y revisar las transacciones que se hicieron en una fecha determinada explorando todos los bloques generados en la fecha indicada.

Las operaciones de consulta no se almacenan en la cadena de bloques por lo que no son auditables mediante la consulta de la cadena de bloques. Cada nodo responde a la consulta de información que se le envía, al no registrarse esta consulta en la cadena, resulta imposible conocer todas las consultas que se realizan en todos los nodos.

En *blockchain* todas **las transacciones consolidadas se guardan en la cadena de bloques**. Esta cadena crece de tamaño constantemente y es almacenada de forma completa por un gran número de nodos que componen la red *blockchain*. Esta característica de *blockchain* hace que toda la información que se procesa sea trazable, pudiendo consultar todas las operaciones realizadas utilizando un explorador de blockchain.

Privacidad

Esta característica es propia de los *blockchain* públicos, donde las **direcciones *blockchain* no están ligadas a las identidades de las personas** que controlan cada una de las direcciones *blockchain*.

Para poder operar en un *blockchain* público es necesario disponer del par de claves pública y privada que permiten controlar la dirección *blockchain*.

La operación que permite generar el conjunto de claves y la dirección de un *blockchain* es un proceso sencillo que se realiza utilizando funciones matemáticas y se puede ejecutar desde el *software* de la solución *blockchain* (*bitcoin*, *ethereum*, etc.) o en internet utilizando el servicio proporcionado por empresas que permiten realizar operaciones en *blockchain* como las casas de cambio (*exchange*).

El proceso que permite generar las claves y la dirección no requiere de ningún dato personal, por lo que la dirección y las claves no van asociadas a la identidad de la persona que crea la dirección. Este mecanismo para proporcionar una dirección de *blockchain* proporciona privacidad a la hora de operar dentro de la red *blockchain*, ya que las transacciones van asociadas a una dirección y firmadas con una clave que no tienen asociado datos sobre la identidad de la persona que realiza la transacción.

Esta característica de *blockchain* no está disponible en todas las distribuciones, ya que, en algunos casos, para poder operar sobre una red *blockchain* se requiere una identificación previa.

La privacidad es una de las principales características de los *blockchain* públicos y otro de los motivos del éxito de blockchain en sus inicios, ya que, en algunos casos, esta privacidad fue utilizada por algunas personas para realizar operaciones consideradas ilegales. Este es uno de los motivos que hicieron que algunos países rechazaran el uso de *blockchain* como medio de pago.

La privacidad ofrecida por *blockchain*, no implica que no se pueda identificar [1] a la persona que realiza cierto tipo de transacciones. En algunos casos la policía ha investigado ciertas operaciones sospechosas y ha conseguido identificar a la persona que realizaba las operaciones gracias a los datos de los proveedores de telecomunicaciones y los patrones de comportamiento de la persona.

Transparencia

La transparencia en blockchain se consigue publicando las reglas con las que se define el funcionamiento de *blockchain*. Esto se logra haciendo **público el código del software necesario para ejecutar *blockchain*** y generando una comunidad de nodos y desarrolladores que siguen este principio de transparencia.

Confianza

La confianza en el funcionamiento de *blockchain* es la característica que hace que dos personas que no confían entre sí puedan realizar una transacción en *blockchain*.

Funcionamiento de blockchain

La secuencia de pasos que permiten generar, enviar y ejecutar una transacción [2] en *blockchain* se muestra en la figura 1 y requiere de un conjunto de pasos donde intervienen los elementos que se presentan en los siguientes puntos.

Figura 1. Los pasos de creación, envió y ejecución de una transacción.

Dirección *blockchain*

Para poder operar en *blockchain* es necesario disponer de una dirección.

Una **dirección *blockchain* es un identificador** único con un tamaño determinado que se construye [3] partiendo de la clave pública y aplicando unas funciones hash determinadas. En el caso de bitcoin el resultado es un identificador alfanumérico que tiene como máximo 35 caracteres. En ethereum la dirección empieza con "0x" seguido de 40 caracteres hexadecimales.

- **Ejemplos de direcciones:**
  - **Bitcoin:** 127NVqnjf8gB9BFAW2dnQeM6wqmy1gbGtv
  - **Ethereum:** 0xFAc399E49F5B6867AF186390270AF252E683b154

Como se observa en las direcciones de ejemplo cada *blockchain* establece un formato o tamaño diferente para la dirección y en este caso las direcciones de *bitcoin* no son compatibles con las direcciones de *ethereum*, lo que quiere decir que no se puede utilizar una dirección de *ethereum* para realizar una transacción en *bitcoin*.

Transacción

Las **operaciones con *blockchain* se realizan mediante el envío de transacciones**. La operativa más simple contemplada en una transacción implica el envío de una cantidad de criptomoneda de una dirección *blockchain* origen, a una dirección *blockchain* destino. Como se ve en la siguiente representación de los principales elementos que componen una transacción *(figura 2)*.

Figura 2. Principales elementos de una transacción.

Para poder enviar una transacción es necesario contar con una dirección *blockchain*, el conjunto de claves asociadas a la dirección y saldo suficiente para poder pagar los costes de ejecución de la transacción.

El **coste de ejecución de una transacción** se divide en dos partes:

- Por un lado, está la cantidad de criptomoneda que se quiere enviar a la dirección destino. Es necesario que la dirección origen disponga de saldo suficiente, de lo contrario la transacción es rechazada.
- Por otro lado, es necesario costear el procesado de la transacción, para lo cual se paga una tarifa que supone una cantidad muy pequeña y que tiene como objetivo recompensar al nodo de la red por procesar la transacción.

Si se quiere priorizar la ejecución de una transacción, para que sea procesada en menor tiempo, el emisor ha de incrementar la cuantía que se paga por la ejecución de la transacción.

Firma de transacciones

Tras definir la transacción, es necesario **firmar los datos que se envían** en la transacción con la **clave privada**, este paso permite generar la firma digital o sello que establecer la autenticidad de los datos de la transacción *(figura 3)*.

Para **verificar la autenticidad de la transacción** y sus datos, se comprueba la firma utilizando la **clave pública** y los datos de la transacción, de manera que se verifica que **solo el poseedor de la clave privada** asociada a la clave pública ha podido **generar la firma** incluida en la transacción para los datos enviados.

A los principales elementos que forman una transacción, se añade la firma digital *(figura 4)*.

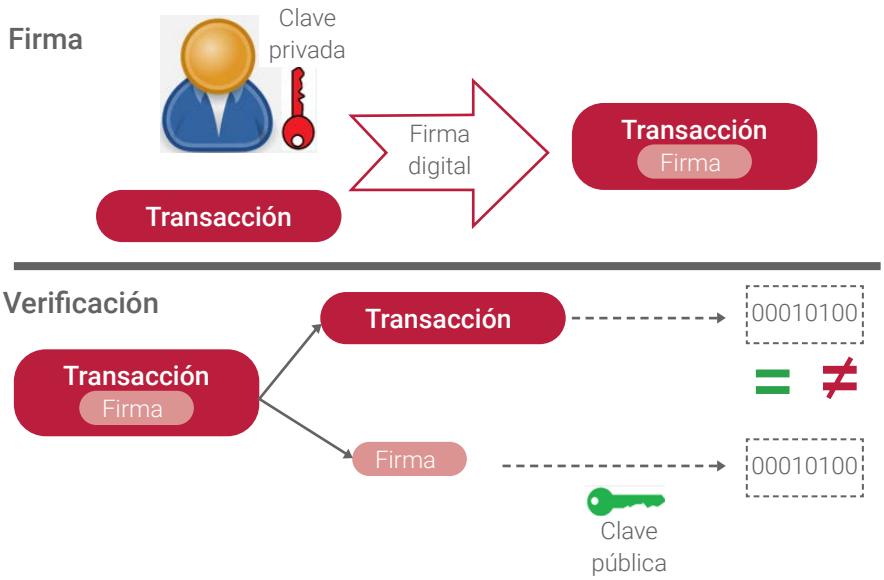

Figura 3. Firma y verificación de una transacción.

Figura 4. Principales elementos de una transacción firmada.

Red P2P

Los ordenadores que tienen instalado el *software* de la distribución de *blockchain* y que están conectados a la red se denominan nodos. Son los responsables de recibir las transacciones y de p**ropagar las transacciones entre la red de nodos** detectados, permitiendo que la transacción llegue a todos los nodos de la red.

La red que utiliza *blockchain* es del tipo *peer-to-peer* y permite la comunicación entre nodos sin la necesidad de un servidor centralizado. En la introducción a *blockchain* se presentaron distintas tipologías de redes P2P *(figura 5)*, siendo la más utilizada en *blockchain* la red denominada pura, donde todos los nodos ejercen como clientes y como servidores.

Esta red P2P permite que la transacción que se envía a un nodo o a un conjunto limitado de nodos pueda extenderse por toda la red *blockchain*.

En ***blockchain* existen dos tipos de nodos**:

- **Nodos:** mantienen la cadena de bloques y propagan las transacciones por la red.
- **Mineros:** realizan las mismas funciones que un nodo, además procesan las transacciones y son los encargados de generar nuevos bloques.

Mineros

Los mineros son un tipo de nodo dedicado a ejecutar las transacciones y a incluirlas en un bloque.

Las transacciones que primero selecciona un minero de *bitcoin* o de *ethereum*, son las que más recompensa proporcionan, de esta manera las transacciones que pagan una cantidad mayor por su ejecución se procesa antes.

En *bitcoin* y *ethereum* todos los nodos mineros compiten entre sí para generar un bloque que pueda ser elegido ganador. El bloque ganador se envía al resto de nodos para que verifiquen si es el ganador de la competición. Solo el bloque declarado como ganador es el que se añade a la cadena de bloques.

Cada *blockchain* establece un tiempo aproximado para incorporar un nuevo bloque a la cadena. En *bitcoin* se incorpora un nuevo bloque a la cadena aproximadamente cada 10 minutos.

En la competición, cada minero intenta crear un bloque con un conjunto de transacciones. El bloque que genera el nodo A puede tener distintas transacciones que el bloque que genera el nodo B.

El ganador de la competición se determina con base en el algoritmo de consenso utilizado en la distribución de *blockchain*.

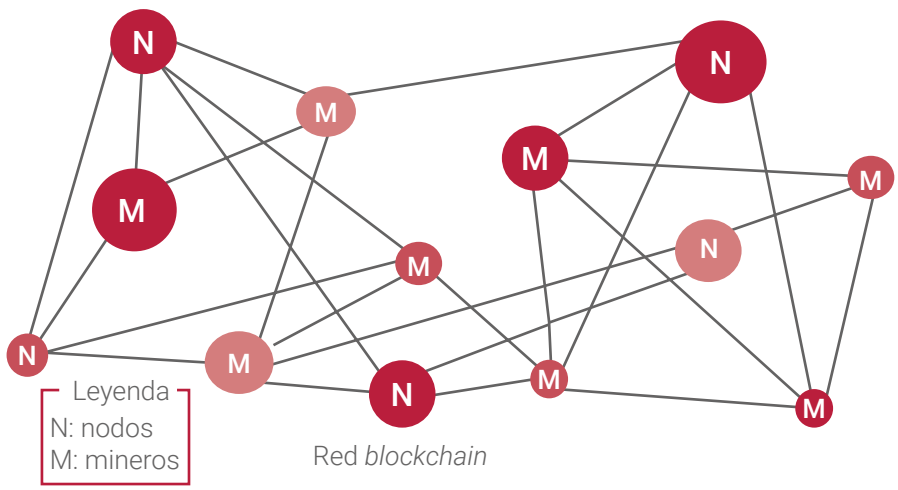

Figura 5. Red *blockchain* de nodos y mineros.

Cada vez que un nodo minero publica un bloque que cumple el reto y es declarado ganador recibe una recompensa. La recompensa varía en función de la distribución de *blockchain* y suele ser una cantidad de la criptomoneda. Esta recompensa incentiva a los nodos mineros a participar en la competición, ya que el valor que se recibe suele ser una cantidad considerable de dinero.

El minero que consigue minar un bloque también recibe las tarifas pagadas por la ejecución de las transacciones incluidas en el bloque.

Cuando se declara un bloque ganador y se añade a la cadena de bloques, los mineros eliminan de la lista de transacciones a procesar las que se han incluido en el bloque ganador y comienza de nuevo la competición por generar un nuevo bloque ganador.

Bloques

Un bloque contiene un listado de transacciones ejecutadas por un minero y otra información como la referencia al identificador del bloque anterior, el número secuencial que identifica al bloque, la versión *blockchain* y la fecha o *time stamp*. Los bloques incluyen mucha más información dentro de la cabecera, pero los elementos esenciales se muestran en la *(figura 6)* donde se representa la cadena que van generando los bloques al incluir la referencia al bloque anterior.

Algoritmo de consenso

Determina las reglas que permiten seleccionar el bloque que se añade a la cadena de bloques.

Dado que existe una gran variedad de algoritmos de consenso y que este contenido se va a tratar con mayor profundidad en el próximo tema, en este punto solo se presenta el algoritmo de *proof of work* o prueba de trabajo, que es el que se utiliza en *bitcoin* y el primer algoritmo de consenso utilizado en *blockchain*.

La prueba de trabajo establece un reto variable que los mineros han de resolver para poder presentar el bloque ganador.

El reto consiste encontrar un número resultante de aplicar una función *hash* a los datos incluidos en el bloque, de manera que el resultado sea menor que el número definido para el reto.

Para poder entender esta definición al completo, se presenta una secuencia de los pasos necesarios para resolver el reto mediante un ejemplo:

- Como ya se ha explicado cada minero selecciona y procesa un conjunto de transacciones para generar el contenido de un bloque. Cuando el bloque está lleno de transacciones se calcula el número del reto utilizando el valor incluido en el campo '*difficulty target*' *(figura 7)*.

  Para este ejemplo se propone que el número del reto es Z.

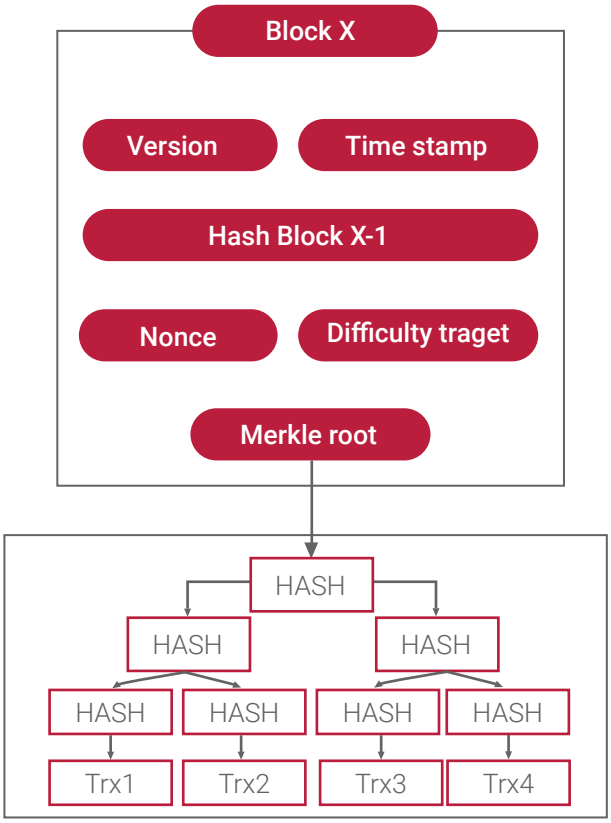

Figura 7. Esquema contenido de un bloque.

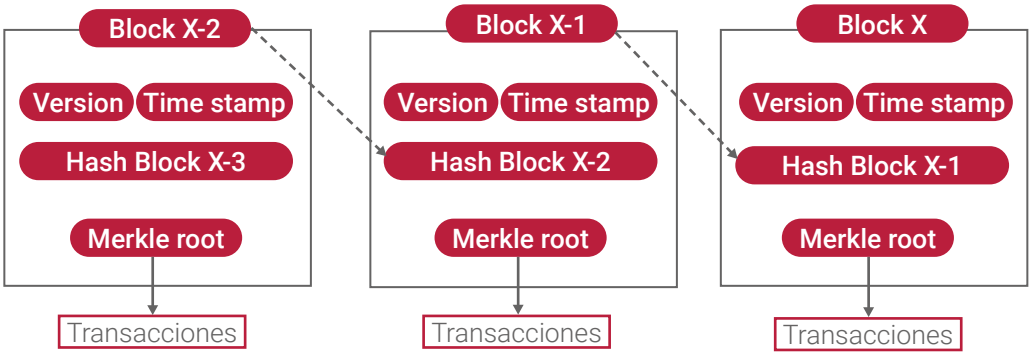

Figura 6. Esquema cadena de bloques.

- El siguiente paso consiste en aplicar una función hash al contenido de bloque y comprobar si el número obtenido X es menor que el número del reto calculado anteriormente Z.

  - Hash(bloque)=X

  Se comprueba si X<Z.

- Pero qué ocurre si al aplicar la función *hash* el número obtenido X no es menor que Z. Como la función *hash* se aplica sobre el contenido del bloque, es necesario modificar este contenido para obtener otro número X1. Esto se consigue cambiando el contenido de un campo llamado "*nonce*" que se encuentra dentro del bloque y que va a permitir generar un nuevo número llamado X1.

  - Hash(bloque)=X1

  De nuevo se comprueba si X1<Y, si no se cumple, se vuelve a repetir el proceso, hasta que se cumple la condición y se publica el bloque que cumple el reto.

- Este proceso lo realizan todos los nodos mineros a modo de competición, donde solo se selecciona un bloque ganador. El nodo que consigue generar el bloque ganador recibe la recompensa y el pago correspondiente a la ejecución de las transacciones incluidas en el bloque.

En *bitcoin* la dificultad de la prueba de trabajo se ajusta para que de media se genere un bloque ganador cada 10 minutos.

Es posible que en una red muy grande dos mineros publiquen un bloque ganador al mismo tiempo y que en el proceso de validación, cada uno de los bloques cuente con la aprobación de otros nodos. En este caso, lo que ocurre es que se genera un '*fork*' o ramificación de la cadena. Este es un comportamiento gestionado por *blockchain* mediante unas reglas que permiten seleccionar una de las ramas para formar parte de la cadena, mientras que la otra rama se deshace, incorporando las transacciones de los bloques de la rama no seleccionada al listado de transacciones pendientes, siempre que no hayan sido procesadas e incluidas en algún bloque de la rama consolidada.

Las transacciones incluidas en el último bloque de la cadena, no pueden considerarse como definitivas, es posible que el bloque se deseche por causa de un *fork* o por detectar un doble gasto. Cada nuevo bloque que se añade a la cadena refuerza el contenido de los bloques anteriores. En *bitcoin* se define la profundidad de la cadena al número de bloques posteriores a un bloque dado. Ejemplo, si se envía una transacción y se mina en el bloque 24, cuando se incluye el bloque 25 a la cadena la profundidad de la transacción enviada es 1. Cada nuevo bloque añadido incrementa la profundidad. En *bitcoin* [4] se recomienda esperar a que la transacción cuente con una profundidad de 6 bloques para considerar que ha sido consolidada. En *ethereum* se recomienda contar con una profundidad de 12 bloques.

Resumen

Hablar de una tecnología segura, trazable, que genere confianza y que proporcione confianza y privacidad, es hablar de *blockchain*. Estas características que proporciona la tecnología de la cadena de bloques son un reclamo para muchas empresas, que actualmente están explorando la aplicación de la tecnología *blockchain* dentro de las particularidades del negocio y de la empresa.

El funcionamiento de blockchain se centra en el procesado de transacciones y se rodea de otros elementos como la dirección *blockchain*, la firma digital y la red P2P que permiten crear la transacción y propagarla por la red *blockchain*. La función de procesar las transacciones recae sobre los mineros que han de competir para generar el bloque que sea declarado ganador y por tanto incluido en la cadena de bloques. La incorporación en la cadena ha de ser aceptada por los nodos siguiendo las rejas definidas por el algoritmo de consenso.

Bibliografía

[1] J. Bohannon Mar. (2016, 9 de marzo). *Por qué los criminales no pueden esconderse detrás de bitcoin*. [En línea]. Disponible en: https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

[2] A. M. Antonopoulos. (2014, diciembre). *dominando bitcoin*. O´Reilly Media, Inc. [En línea]. Disponible en: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html

[3] T. Tore. (2020, enero 15). *Cómo generar una dirección bitcoin: explicación técnica de la generación de direcciones*. [En línea]. Disponible en: https://hackernoon.com/how-to-generate-bitcoin-addresses-technical-address-generation-explanation-rus3z9e

[4] (2018). "*Confirmación*". [En línea]. Disponible en: https://en.bitcoin.it/wiki/Confirmation