INVESTIGA I+D+i 2018/2019

GUÍA ESPECÍFICA DE TRABAJO SOBRE "TECNOLOGÍA BLOCKCHAIN

Texto de D. Francisco Javier Cárceles Moreno

Octubre de 2018

Introducción

Como sucede, desde que la informática aparece en la vida del ser humano, se van produciendo **avances** de manera continua. Uno de los últimos ha sido la creación e implantación de la **cadena de bloques** o **blockchain**.

Fruto de la iniciativa de unos programadores, que en los años 90 definen una solución para la realización de **pagos electrónicos**, nace la cadena de bloques o blockchain, que serviría en aquel entonces y en la actualidad, para **crear monedas electrónicas** o criptomonedas y para **otras funciones** que utilizan esta tecnología.

La cadena de bloques o blockchain es un avance reconocido mundialmente como la **quinta evolución de la informática**.

¿Qué es la cadena de bloques? y ¿qué tecnología usa?.

La cadena de bloques es una tecnología que se basa en tres pilares.

- Unas estructura de datos organizada en unidades llamada **bloques**.
- La encriptación de los **enlaces** de la cadena para que no pueda ser descifrada o cambiada.

- Una red de **nodos** que se encargan de la gestión, creación y validación de la estructura de los datos.

Estos tres pilares son soportados por **programas informáticos** que, en cada uno de ellos, cubren todas las funcionalidades requeridas.

¿Para qué sirve cada una de las partes de la cadena de bloques o blockchain?

- **Bloque**: es el componente que guarda los **datos asociados a una transacción** de criptomoneda, relativa a un **contrato inteligente** o a **otro tipo de datos** que se puedan guardar en formato electrónico.

  Cada uno de los bloques **contiene información del bloque anterior,** de manera que esta información también forma parte del bloque. Está peculiaridad permite que no se pueda cambiar el contenido de un bloque sin alterar la cadena por completo.

  Los datos que se almacenan en cada bloque pueden ser de diversa naturaleza. En el entorno de las monedas virtuales o criptomonedas sirven para indicar quién es el **poseedor** de una de ellas, en entornos Ethereum sirven para que las partes que quieran **firmen acuerdos** a través de **contratos inteligentes**. Cualquier dato que quede registrado en el bloque podrá ser consultado por los usuarios, gracias a la **criptografía asimétrica**.

- **Cadena** o enlace: es un **hash** o codificación generada por criptografía que **une dos bloques** y que es creado a partir de los datos que están contenidos en el bloque anterior. De esta forma el código es único y significa una **huella digital** de estos datos, bloqueándolos en el **tiempo** y en la **posición** del bloque.

  Cada hash se crea de una información de inicio que será el **contenido del bloque anterior** excepto el primero de la cadena que es creado sin esa característica. Estos hash son creados por **programas criptográficos** que consumen mucho tiempo de

ejecución pues necesitan realizar **muchas operaciones matemáticas**. La idea entonces es que los nodos ayuden a crear estos hash y consigan una recompensa, en modo de monedas generalmente, para que sigan ayudando a su generación.

Tal es la potencia y tiempo usado en la generación de hash por los nodos que para poder conocer la información de partida partiendo del hash, un solo ordenador estaría años haciendo cálculos y no lo conseguiría.

La **modificación** de cualquiera de los **bloques** que conforman la cadena revelaría que la información **no es correcta** por lo que se deben rechazar los nodos que soportan la cadena modificada.

- **Red de nodos**: está formada por la red de ordenadores que contienen una **copia del blockchain** y **generan formas digitales**, **aprueban transacciones** y las **registran** en la cadena.

  La red que forman los nodos o equipos que trabajan para la cadena se basa en **tecnología P2P (Peer to Peer)**, que es una red en donde no hay servidores y todos los equipos funcionan como iguales.

  Está red sirve para que los nodos que crean los bloques y los validan **colaboren** entre sí **intercambiando** la información necesaria. El proceso por el cual se validan los bloques se llama **POW (Proof-Of-Work)** y se basa en la validación del bloque por parte de los nodos que están trabajando en la red P2P.

Pero entonces ¿cualquiera puede escribir en la cadena y leer de ella?.

La cadena de bloques es una estructura de datos que **no está centralizada** y por lo tanto su soporte se basa en una **comunidad de usuarios** que la tienen en sus ordenadores compartida. Algunos de estos usuarios ayudan a crear los bloques y guardarlos una vez que la comunidad los valida. Por lo tanto si el blockchain no es privado no pertenece a nadie aunque depende de que muchas personas ayuden a su mantenimiento y creación.

Las personas que tengan el **software cliente** podrán visualizar los datos de la cadena si tienen los permisos adecuados para ello. También podrán usarla realizando, a través de los programas de la cadena, las **transacciones** o **operaciones** permitidas por dicho software.

¿Cuántos tipos de blockchain se conocen?

Existen varios tipos de cadenas de bloques en relación a su acceso:

1. **Públicas** que son compartidas en Internet y que suelen ser producidas por un software libre y compartido. Un ejemplo podría ser la que gestiona los **bitcoins** o **Ethereum**.
2. **Protegidas** que son accesibles a través de una credencial y el uso que se haga de ella dependerá del nivel de acceso obtenido. Un ejemplo de ellas es **Ripple**.
3. **Privadas** que suelen ser muy pequeñas y funcionan dentro de un consorcio o entidad.

También hay cadenas que están construidas para determinados tipos de fines tales como:

1. **Criptomonedas**, la gran mayoría de blockchain se usan para producir y gestionar monedas virtuales como bitcoin, Litecoin, Dash, etc…
2. **Contratos inteligentes (Smart Contracts)**, su finalidad es que los acuerdos realizados y registrados por dos o más partes se ejecuten. Los contratos inteligentes son programas que **evalúan el cumplimiento del acuerdo** y efectúan las operaciones programadas que se acordaron por las partes. Una operación podría ser ingresar bitcoins en una wallet o monedero electrónico.
3. **Otras funciones**, como hemos visto la cadena de blockchain actúa como un libro de registros de operaciones. Estos registros que son validados por la comunidad sirven para multitud de operaciones específicas como podrían ser: registros notariales, registros de la propiedad intelectual, trazabilidad de productos, automatización de procesos, etc..

Conceptos y cuestiones de debate.

Después de ver las características del blockchain a nivel funcional propongo que, para poder avanzar en la investigación se estudien los siguientes conceptos y se respondan a las siguientes cuestiones:

Conceptos:

1. Criptografía, Fingerprint, Hash,Timestamp .
2. Algoritmos de consenso y prueba de trabajo
3. Criptomonedas.
4. Minería de blockchain.
5. Contratos inteligentes.
6. Aplicaciones distribuidas.

Preguntas:

1. ¿Cómo funciona el blockchain de bitcoin?
2. ¿Cómo funciona el blockchain de Ethereum?
3. ¿Cómo funciona el blockchain de Ripple?
4. Si el blockchain es una base de datos distribuida y reconciliada, ¿cuales serían los sectores en los que su uso sería un valor añadido?
5. ¿Es la cadena de bloques o blockchain un intermediario fiable?, ¿por qué?
6. La suma de la potencia de los ordenadores que forman los nodos en la red es muy elevada, ¿crees que es un inconveniente para implantar blockchain? y si lo es, ¿cuáles serían los proyectos en donde dicha potencia no sería un inconveniente?
7. En definitiva ¿cuáles podrían ser los usos futuros para esta tecnología?

Fuentes de información

- Blockchain For Dummies®, Published by: John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774
- The Science of the Blockchain Roger Wattenhofer, Inverted Forest Publishing
- "Blockchain Revolution" Tapscott, Don. "Penguin Random House LLC 375 Hudson Street New York, New York 10014"
- https://learn.unimooc.com/student/courses/course?course=bitcoin;utm_source=desktop&utm_medium=txt
- https://es.wikipedia.org/wiki/Ethereum
- https://es.wikipedia.org/wiki/Cadena_de_bloques
- https://ripple.com/