Blockchain

Autor 1: John Sebastián Luján Figueroa
Risaralda, Universidad Tecnológica de Pereira, Pereira, Colombia
Correo-e: s.lujan@utp.edu.co

***Resumen*— ¿Qué es el blockchain? Entre otras cosas, es una de las palabras de moda en los últimos tiempos. La cadena de bloques es también un concepto que plantea una enorme revolución no solo en nuestra economía, sino en todo tipo de ámbitos.**

Entender lo que es esa cadena de bloques no es tan difícil, y dado que cada vez se utiliza más este concepto hemos querido hacer una especie de curso rápido de introducción al blockchain, para explicar qué es, cómo funciona y cuál es esa revolución que plantea la cadena de bloques.

***Palabras clave*— blockchain, nonce, hash, registro.**

***Abstract*— What is the blockchain? Among other things, it is one of the buzzwords of recent times. The chain of blocks is also a concept that raises a huge revolution not only in our economy, but in all kinds of areas.**

Understanding what this chain of blocks is is not so difficult, and since this concept is being used more and more, we wanted to make a kind of quick introduction to the blockchain, to explain what it is, how it works and what that revolution is the chain of blocks.

***Key Word* — blockchain, nonce, hash, registry.**

I. INTRODUCCIÓN

Una cadena de bloques, conocida en inglés como blockchain, es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en entorno distribuido de manera que la estructura de datos blockchain puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información.7En la práctica ha permitido, gracias a la criptografía asimétrica y las funciones de resumen o hash, la implementación de un registro contable (ledger) distribuido que permite soportar y garantizar la seguridad de dinero digital.8 Siguiendo un protocolo apropiado para todas las operaciones efectuadas sobre la blockchain, es posible alcanzar un consenso sobre la integridad de sus datos por parte de todos los participantes de la red sin necesidad de recurrir a una entidad de confianza que centralice la información. Por ello se considera una tecnología en la que la "verdad" (estado confiable del sistema) es construida, alcanzada y fortalecida por los propios miembros; incluso en un entorno en el que exista una minoría de nodos en la red con comportamiento malicioso (nodos sybil) dado que, en teoría, para comprometer los datos, un atacante requeriría de una mayor potencia de cómputo y presencia en la red que el resultante de la suma de todos los restantes nodos combinados. Por las razones anteriores, la tecnología blockchain es especialmente adecuada para escenarios en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora. Este enfoque tiene diferentes aspectos:

- Almacenamiento de datos: se logra mediante la replicación de la información de la cadena de bloques
- Transmisión de datos: se logra mediante redes de pares.
- Confirmación de datos: se logra mediante un proceso de consenso entre los nodos participantes. El tipo de algoritmo más utilizado es el de prueba de trabajo en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada minería.

El concepto de cadena de bloque fue aplicado por primera vez en 2009 como parte de Bitcoin.

Los datos almacenados en la cadena de bloques normalmente suelen ser transacciones (p. ej. financieras) por eso es frecuente llamar a los datos transacciones. Sin embargo, no es necesario que lo sean. Realmente podríamos considerar que lo que se registran son cambios atómicos del estado del sistema. Por ejemplo una cadena de bloques puede ser usada para estampillar documentos y asegurarlos frente a alteraciones.

II. CONTENIDO

Fecha de Recepción: (Letra Times New Roman de 8 puntos)
Fecha de Aceptación: Dejar en blanco

Aplicaciones

El concepto de cadena de bloques se usa en los siguientes campos:

- En el campo de las criptomonedas la cadena de bloques se usa como notario público no modificable de todo el sistema de transacciones a fin de evitar el problema de que una moneda se pueda gastar dos veces. Por ejemplo es usada en Bitcoin, Ethereum, Dogecoin y Litecoin, aunque cada una con sus particularidades.
- En el campo de las bases de datos de registro de nombres la cadena de bloques se usa para tener un sistema de notario de registro de nombres de tal forma que un nombre solo pueda ser utilizado para identificar el objeto que lo tiene efectivamente registrado. Es una alternativa al sistema tradicional de DNS. Por ejemplo es usada en Namecoin.
- Uso como notario distribuido en distintos tipos de transacciones haciéndolas más seguras, baratas y rastreables. Por ejemplo se usa para sistemas de pago, transacciones bancarias (dificultando el lavado de dinero), envío de remesas, préstamos y en los sistemas de gestión de activos digitales puede ser usado con distintos propósitos.
- Es utilizado como base de plataformas descentralizadas que permiten soportar la creación de acuerdos de contrato inteligente entre pares. El objetivo de estas plataformas es permitir a una red de pares administrar sus propios contratos inteligentes creados por los usuarios. Primero se escribe un contrato mediante un código y se sube a la cadena de bloques mediante una transacción. Una vez en la cadena de bloques el contrato tiene una dirección desde la cual se puede interactuar con él. Ejemplos de este tipo de plataformas son Ethereum y Ripple.
- Implementación del componente criptográfico llamado Bulletin Boards usado, entre otros, en sistemas de voto electrónico, creación de registros, subastas y foros de discusión.

Clasificación

Según el acceso a los datos

Las cadenas de bloques se pueden clasificar basándose en el acceso a los datos almacenados en la misma:

- Cadena de bloques pública: es aquella en la que no hay restricciones ni para leer los datos de la cadena de bloques (los cuales pueden haber sido cifrados) ni para enviar transacciones para que sean incluidas en la cadena de bloques. En ellas es fácil entrar y salir, son transparentes, están construidas con precaución para la operación en un entorno no confiable. Son ideales para uso en aplicaciones totalmente descentralizadas como por ejemplo para el Internet.
- Cadena de bloques privada: es aquella en la que tanto los accesos a los datos de la cadena de bloque como el envío de transacciones para ser incluidas, están limitadas a una lista predefinida de entidades.

Ambos tipos de cadenas deben ser considerados como casos extremos pudiendo haber casos intermedios.

Según los permisos

Las cadenas de bloques se pueden clasificar basándose en los permisos para generar bloques en la misma:

- Cadena de bloques sin permisos: es aquella en la que no hay restricciones para que las entidades puedan procesar transacciones y crear bloques. Este tipo de cadenas de bloques necesitan tókenes nativos para proveer incentivos que los usuarios mantengan el sistema. Ejemplos de tókenes nativos son los nuevos bitcoines que se obtienen al construir un bloque y las comisiones de las transacciones. La cantidad recompensada por crear nuevos bloques es una buena medida de la seguridad de una cadena de bloques sin permisos.
- Cadena de bloques con permisos: es aquella en la que el procesamiento de transacciones está desarrollado por una predefinida lista de sujetos con identidades conocidas. Por ello generalmente no necesitan tókenes nativos. Los tókenes nativos son necesarios para proveer incentivos para los procesadores de transacciones. Por ello es típico que usen como protocolo de consenso prueba de participación.

Posibles combinaciones de acceso y permisos

Las posibles combinaciones de ambos tipos de características son:

- Cadenas de bloques públicas sin permisos. Un ejemplo de estas es Bitcoin. Como no es posible la existencia de cadenas de bloques privadas sin permisos, a estas también se las llama simplemente cadenas de bloques sin permisos.
- Cadenas de bloques públicas con permisos. Un ejemplo de estas son las cadenas laterales federadas. Estas cadenas no pueden tener ataques Sybil, por lo que en principio poseen un grado más alto de escalabilidad y flexibilidad frente a las públicas sin permisos.
- Cadenas de bloques privadas con permisos.

Esta combinación es posible ya que hay distintas formas de acceder a los datos de la cadena:

- Leer las transacciones de la cadena de bloques, quizás con algunas restricciones (p. ej. un usuario puede tener acceso solo a las transacciones en las que está involucrado directamente)
- Proponer nuevas transacciones para la inclusión en la cadena de bloques.

- Crear nuevos bloques de transacciones y añadirlo a la cadena de bloques.

Esta combinación es posible ya que hay distintas formas de acceder a los datos de la cadena:

- Leer las transacciones de la cadena de bloques, quizás con algunas restricciones (p. ej. un usuario puede tener acceso solo a las transacciones en las que está involucrado directamente)
- Proponer nuevas transacciones para la inclusión en la cadena de bloques.
- Crear nuevos bloques de transacciones y añadirlo a la cadena de bloques.

La última forma de acceso está restringida para cierto conjunto limitado de entidades. Sin embargo las otras dos formas de acceso no tienen por qué estar restringidas. Por ejemplo una cadena de bloques para entidades financieras sería una cadena con permisos pero podría:9

- Garantizar el acceso de lectura (quizá limitada) para transacciones y cabeceras de bloques para sus clientes con el objetivo de proveer una tecnológica, transparente y fiable forma de asegurar la seguridad de los depósitos de sus clientes.
- Garantizar acceso de lectura completo a los reguladores para garantizar el necesario nivel de cumplimiento.
- Proveer a todas las entidades con acceso a los datos de la cadena de bloques una descripción exhaustiva y rigurosa del protocolo, el cual debería contener explicaciones de todas las posibles interacciones con los datos de la cadena de bloques.

Según modelo de cambio de estado

Las cadenas de bloques también se pueden clasificar según el modelo de cambio de estado en la base de datos en:

Basado en el gasto de salidas de transacciones, también llamado modelo UTXO (en referencia a los UTXO de Bitcoin). En ellas cada transacción gasta salidas de transacciones anteriores y produce nuevas salidas que serán consumidas en transacciones posteriores. A este tipo de cadenas de bloques pertenecen por ejemplo las de Bitcoin, R3, Blockstream, BOSCoin y Qtum. Este enfoque tiene ventajas como:

- En la propia estructura de la cadena existe una prueba de que nunca se puede gastar dos veces ya que cada transacción prueba que la suma de sus entradas es más grande que la suma de sus salidas.
- Cada transacción puede ser procesada en paralelo porque son totalmente independientes y no hay conflictos en las salidas.

Sin embargo el problema de este tipo de cadenas es que solo son utilizables para aplicaciones donde cada salida es propiedad de uno y solo un individuo como por ejemplo es el caso de las monedas digitales. Una salida multipropietario sería muy lenta y no sería eficiente para aplicaciones de propósito general. Por ejemplo, supongamos un contrato inteligente que implementa un contador que puede ser incrementado. Imagina que hay algún incentivo económico para que cada nodo incremente en uno el contador, y que hay 1000 nodos activamente intentado incrementarlo. Usando este modelo de cadena de bloques tendríamos una salida con el valor del contador que sería solicitada por muchos nodos. Finalmente un nodo tendría éxito y produciría una transacción con una nueva salida con el contador incrementado en una unidad más. El resto de nodos estarían forzados a reintentar hasta que su transacción sea aceptada. Este sistema es muy lento e ineficiente. Esto es debido a que un cuando se realiza la transacción se bloquea la salida, se realiza una transformación y finalmente se produce la nueva salida. Esta claro que sería mucho más óptimo si se realizara todo de una sola vez y se produjera directamente el estado resultante. Además el problema puede estar no solo en el tiempo de la transacción, sino también en el de proceso. Supongamos que el contador tiene adjunto un buffer de 1MB cuyo valor cambia de forma determinista cada vez que el contador cambia. Se tendría que procesar 1MB cada vez que realizara una transacción.

Basado en mensajes. En este caso, la cadena de bloques representa un consenso sobre el orden de los mensajes y el estado es derivado de forma determinísta a partir de estos mensajes. Este enfoque es utilizado por las cadenas de bloques de Steem y Bitshares. Por ejemplo para implementar un contador cada usuario debería simplemente firmar un mensaje pidiendo el incremento en uno. No se necesita saber el estado actual del contador para que el mensaje sea válido. En este modelo si 1000 nodos envían la petición al mismo tiempo, el productor del bloque podría agregar todas la peticiones en un bloque y en un solo paso el contador pasaría de valer de cero a valer 1000. Una aplicación del mundo real que aprovecharía las cualidades de este modelo sería el siguiente:

Se emite una orden de compra de productos financieros indicando un precio máximo y un volumen concreto. A partir de ahí hay una competición sobre esa salida entre los participante que quieren la solicitud al mismo tiempo. Supongamos que se desea realizar la transacción de forma que sea lo más beneficiosa posible realizando una subasta a la baja para que la solicitud compre activos por el menor precio.

1. Las notas de pie de página deberán estar en la página donde se citan. Letra Times New Roman de 8 puntos