Published on *Hoy en el TEC* (https://www.tec.ac.cr/hoyeneltec)

Ilustración del concepto de la tecnología Blockchain. Tomada de vecteezy.com [1].

Experto dice que se trata de una nueva era de Internet

Entrevista: ¿Qué es Blockchain y la minería de cripto activos?

10 de Noviembre 2021 Por: Johan Umaña Venegas [2]

Profesor del TEC responde preguntas comunes sobre estas tecnologías

Casi todos los días en las noticias y en las redes sociales escuchamos términos como Bitcoin o NFT (Non Fungible Token, que es como un vale digital). Poco a poco los cripto activos han empezado a formar parte de la vida cotidiana. Y lo que está detrás de todo esto es la tecnología Blockchain (cadena de bloques), que tiene aplicaciones mucho más allá de las cripto monedas.

Kevin Moraga es docente de Ingeniería en Computación y la Maestría en Gerencia de Tecnologías de Información [3].

Para entender más sobre este tema, el Ing. Kevin Moraga García *MSc*., profesor de la carrera de Ingeniería en Computación [4] en el Centro Académico de Alajuela [5] del Tecnológico de Costa Rica (TEC) [6], y de la Maestría en Gerencia de Tecnologías de Información [3], explica los conceptos de esta nueva tecnología que está revolucionando la forma de hacer transacciones en el mundo.

??¿Qué es y cómo funciona el Blockchain?

Desde su concepción, Internet ha sido una solución descentralizada y por naturaleza resiliente. Propone nuevas formas de organización distintas a las acostumbradas dentro la esfera pública, las ya conocidas jerarquías o sistemas centralizados. Esta tecnología, ha probado su utilidad para la humanidad a través de la era del **"Internet de la Información"**, y se podría caracterizar como el corazón del saber colectivo dentro de la sociedad del conocimiento.

Por otro lado, **Blockchain** corresponde al **siguiente paso evolutivo en la era de la información**, proponiendo una transición hacia el **“Internet del Valor”**. Esta nueva tecnología viene a resolver dos grandes desafíos, el primero de ellos corresponde a **cómo definir cosas únicas** en un contexto donde todo es una copia fiel. Y el segundo desafío, se relaciona a **cómo intercambiar valor entre dos pares** sin la necesidad de un intermediario.

Para comprender el funcionamiento de Blockchain se debe de tener en cuenta tres conceptos fundamentales: **1) Funciones *Hash*, 2) *Ledger* o Libro contable Mayor y 3) Los cheques.**

Se puede hacer una analogía de un *blockchain*, a un libro donde sus hojas son talladas en piedra y lo escrito en cada línea corresponde a transacciones que representan un movimiento de un activo. En dicha transacción se deben incluir **los mismos campos que encontramos en un cheque común**, por ejemplo: quién lo emite, para quién va dirigido, el monto a transar, la fecha, una descripción y, por último, una firma de endoso.

Como es de esperar, cada hoja de piedra podría contener un máximo de líneas o transacciones, por ende, al momento de llenarse en su totalidad, es necesario **“sellar” la página para evitar que se pueda alterar en el futuro**. Es posible compararlo con utilizar un laminado de seguridad que proteja a la hoja, y si se hace un cambio en el escrito, el sello se rompe.

Este **sello se realiza utilizando las funciones de *hash***. Estas funciones reciben todas las palabras escritas en la hoja y generan como salida un valor único, creando así una reseña o resumen de la hoja, como si se tratara de un identificador; en caso que se modificara una única letra, la salida sería completamente diferente.

Esta reseña es almacenada al final de cada hoja a modo de sello, dando la posibilidad que cualquiera pueda comprobar que el valor es original dado un texto inalterado, caso contrario se podría concluir que hubo un cambio.

Luego, cuando se crea un nuevo bloque u hoja, se incluye el sello del bloque pasado, al inicio del nuevo bloque, generando un encadenamiento y una dependencia; y así garantizar la invariabilidad de la información previamente escrita en los bloques anteriores. Volviendo a la analogía del laminado, sería como extender este sello a la siguiente hoja, por lo que una alteración en la primera hoja afectaría el laminado de la segunda también.
Por último, **una copia fiel del libro o *ledger* es almacenada por cada participante de la red**, de forma independiente y distribuida.

[7]

Emprendimiento universitario ofrece minería de cripto activos con energía limpia [7]

¿Qué significa "minería" de cripto activos, como Bitcoin o Ethereum?

En el caso de Bitcoin y Ethereum, que corresponde a la primera y segunda generación de Blockchain, respectivamente, ambos utilizan un mecanismo de consenso llamado **Prueba de Esfuerzo**

(*Proof of Work*, en inglés).

Los mecanismos de consenso son utilizados para definir quién tiene la potestad de escribir el último bloque. Por decirlo de otra manera, todos los participantes tienen una copia exacta del Libro o Ledger y todos pueden leerlo en cualquier momento; sin embargo, solo un participante al tiempo puede escribir las nuevas transacciones en un nuevo bloque.

Como se mencionó anteriormente, al final de cada bloque se sella con un número *hash* a modo de reseña. Pero no es un número *hash* cualquiera, sino que debe cumplir alguna regla definida por la red. Por ejemplo, se podría establecer que la reseña inicie con dos dígitos iguales (Ej.: 00XXXX). Para obtener esta condición es necesario incluir dentro del bloque un campo para la búsqueda de un número adicional, y utilizando la fuerza bruta se prueban desde el valor “0” hasta encontrar alguno que genere el *hash* correcto.

La búsqueda por fuerza bruta de este número, también llamado *nonce* (por sus siglas en inglés), es lo que se llama **minar**.

Este minado fomenta una **competencia por crear el nuevo bloque con las reglas de la red**. Al primero en resolver la prueba de esfuerzo o acertijo, se le concede la potestad de escribir.

¿Por qué se requiere tanto poder computacional en esa tarea de minería?

La regla de cuántos dígitos iguales al inicio del *hash* puede variar, esto con el objetivo de **ajustar la complejidad de la búsqueda del *nonce*.** Entre más dígitos iguales sean requeridos, más poder computacional es necesario.

Por otro lado, hay otros mecanismos de consenso que no requieren una prueba de esfuerzo que defina quién tendrá la potestad de escribir el nuevo bloque, por lo que **el requerimiento de poder computacional con estos mecanismos puede ser mucho menor**. Algunos de los protocolos de consenso alternativos son ***Proof of Stake, Proof of Authority***, entre otros.

¿Cómo funcionan los cripto activos?

Al igual que se pueden tener cheques en distintos tipos de monedas, ya sea cheques en colones, dólares o euros; también es posible **utilizar este mismo mecanismo de transferencia de valor para cualquier tipo de activo**, sin importar el símbolo a utilizar. A este **símbolo normalmente se le llama *token*.**

También es posible representar una serie de *tokens*, o bien un único *token*. Un ejemplo práctico sería: **digitalizar monedas coleccionables del bicentenario, donde la cantidad es limitada o variable** a unos cuantos ejemplares.

Asimismo, existen redes *blockchain* donde no necesariamente se utiliza un *token* y **más bien se almacena directamente un archivo o el *hash* de un archivo**.

¿En qué tipo de bienes o servicios se pueden aplicar estas técnicas computacionales?

Cualquier bien o servicio que pueda ser **digitalizable y necesite las propiedades de trazabilidad, transparencia e inmutabilidad**.

El Ing. Kevin Moraga *MSc*. enseña los cursos de Sistemas Operativos, Redes, Seguridad del Software y Ataque y defensa de sistemas, para la carrera de Ingeniería en Computación [4].

También, Gestión de la Seguridad de la Información, para la Maestría en Gerencia de Tecnologías de Información [3].

Enlaces
[1] https://www.vecteezy.com/vector-art/2180593-blockchain-and-cryptocurrency-technology
[2] https://www.tec.ac.cr/hoyeneltec/users/johan-umana-venegas
[3] https://www.tec.ac.cr/carreras/maestria-gerencia-tecnologias-informacion
[4] https://www.tec.ac.cr/programas-academicos/bachillerato-ingenieria-computacion
[5] https://www.tec.ac.cr/ubicaciones/centro-academico-alajuela
[6] https://www.tec.ac.cr/
[7] https://www.tec.ac.cr/hoyeneltec/2021/11/10/emprendimiento-universitario-ofrece-mineria-cripto-activos-energia-limpia