UN RESUMEN DE LOS COMPONENTES TÉCNICOS DE BLOCKCHAIN Y BITCOIN

FRANCISCOMONTOTO
Egresado de Ingeniería Civil en Computación, Universidad de Chile. Actualmente ayudante de investigación en NIC Chile Research Labs y estudiante de Magíster en Ciencias mención Computación. Posee bitcoins desde 2014 y su tesis de Magíster es sobre traer información del mundo exterior a la Blockchain de Bitcoin mediante oráculos distribuidos. Sus tópicos de interés son la Criptografía, Sistemas Distribuidos, Software de Sistema y Redes.
fmontotomonroy@gmail.com

• La característica revolucionaria de Bitcoin con respecto a soluciones anteriores es, sin dudas, su arquitectura distribuida que le permite prescindir de una autoridad centralizada. Esto lo logra haciendo que todas las transacciones en el sistema sean públicas. La tecnología que hizo posible esto es la columna vertebral de Bitcoin, una base de datos distribuida conocida como "cadena de bloques" (Blockchain).

• Como su nombre lo indica, la cadena de bloques es una secuencia de estos. Con un inicio bautizado como "bloque génesis", y un extremo donde se van agregando nuevos bloques que hacen crecer la cadena. El bloque es la unidad estructural de la base de datos y en él se guarda la información. Los bloques son enlazados vía un cálculo matemático: cada nuevo bloque incluye un hash criptográfico del bloque anterior. Es decir, en el bloque i está incluido el hash del bloque i-1. La función de hash escogida tiene la propiedad de que encontrar un bloque distinto al utilizado que generen el mismo hash es computacionalmente infactible, lo cual efectivamente impide la modificación o reemplazo de un bloque una vez que los nuevos bloques lo referencian.

• Cada bloque tiene un tamaño máximo de datos útiles, donde se almacenan las transacciones. La cadena de bloques es pública y cualquiera puede descargarla en su computador si posee una conexión a Internet, lo cual hace "reconocible" a los bits. Para saber si los bits que recibo como pago son válidos, basta consultar esta base de datos. Esto y el hecho que una vez ingresado un bloque no puede cambiarse es uno de los factores que impide a los usuarios copiar y gastar dos veces una misma moneda.

• Para que un bloque sea aceptado en la cadena, debe tener una prueba de trabajo *(proof of work)*. Esta técnica fue inventada originalmente para combatir el spam de correos electrónicos. Consiste en requerir trabajo antes de aceptar datos provenientes de un tercero. La versión más utilizada consiste en exigir ejecutar una tarea compleja que genera un resultado de fácil validación. Así el receptor puede determinar rápidamente si el remitente efectuó o no el trabajo requerido.

• El proceso de validar transacciones, ponerlas en un bloque y anexar el bloque a la cadena es conocido como "minar". Los mineros son quienes mantienen la integridad de la base de datos y compiten entre ellos para colocar bloques en ésta, pues el creador del bloque es quien recolecta los honorarios *(fees)* de cada transacción en el bloque. Así, un minero es recompensado por cada bloque que agrega a la cadena. La prueba de trabajo consiste en que el valor del hash de cada bloque sea menor a la de un determinado umbral, así el minero debe cambiar el contenido del bloque que intenta minar hasta obtener un hash que cumpla el umbral. Una buena función de hash hace que no exista forma de hacer esto más que por fuerza bruta.

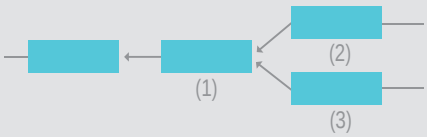

FIGURA 1.

• Naturalmente, que cada minero pueda agregar nodos generará bifurcaciones en la cadena **(Figura 1)**, donde bloques de distintos mineros apunten a un bloque común previo. Esta situación es problemática, pues una moneda disponible en *(1)* puede transferirse a un destinatario A en *(2)* y a un destinatario B en *(3)*, esto se conoce como "doble gasto". Pequeñas bifurcaciones ocurren normalmente en la cadena, y para resolverla solo queda esperar cuál de las dos ramificaciones alcanza un largo mayor, la cadena de consenso es la más larga desde el nodo génesis.

• La cadena de bloques define mayoría en base al poder de cómputo, si una entidad posee más de la mitad del poder de cómputo en la red tendrá el control de ésta. Ésta es la forma de la cadena de bloques para resolver uno de los problemas fundamentales en sistemas distribuidos, el consenso: ¿cómo hacer que los participantes del sistema acuerden un valor? Utilizar el poder de cómputo como métrica hace más difícil -pues es más costoso- un ataque *Sybil* (un atacante creando múltiples identidades para convertirse en mayoría). Ser capaz de tolerar este tipo de ataques es esencial en un sistema de dinero electrónico con participación abierta de entidades anónimas.

• Una transacción en Bitcoin es muy similar a una en otra moneda, es la transferencia de bitcoins entre cuentas. Para que esta transferencia suceda es necesario demostrar que quien hace la transferencia controla la cuenta de origen, y conoce el identificador de la cuenta de destino. Una cuenta es un par de claves público-privada, en un sistema criptográfico asimétrico de Curva Elíptica. Y su identificador, conocido como dirección, es el hash de la clave pública. Para gastar los bitcoins almacenados en una cuenta es necesario revelar la clave pública -la preimagen de la dirección- de la cuenta de origen y demostrar el control sobre ésta, mediante la firma de la transacción con la clave privada. Sin embargo el potencial de las transacciones es bastante mayor a transferir dinero directamente, una transacción puede contener código y establecer distintas condiciones para gastar el monto recibido. Si bien el lenguaje aceptado en Bitcoin es bastante limitado, nuevas monedas -como Ethereum- incorporan lenguajes Turing-Completos, que permiten una expresividad sin precedentes en las condiciones para gastar el dinero, esto permite transacciones que, por ejemplo, obliguen a una parte a realizar una acción para obtener el dinero. Este tipo de acuerdos en monedas electrónicas es uno de sus usos con mayor proyección y se conocen como "Contratos Inteligentes". ■