BLOCKCHAIN

Blockchain es un sistema distribuido cuyo objetivo es proporcionar una plataforma confiable y segura para el manejo de transacciones. El concepto de blockchain fue puesto por primera vez en práctica en la criptomoneda Bitcoin. De hecho, la confiabilidad y confidencialidad que posee esta moneda, se debe a que utiliza el sistema de blockchain para sus transacciones.

Como su nombre lo indica, blockchain consiste en una cadena de bloques donde cada bloque es un conjunto de transacciones y a su vez estos bloques se enlazan con otros bloques en un orden único e inalterable. Debido a este orden único, toda transacción presente en un bloque queda completamente validada y no hay forma de que se pueda falsificar por razones que se explicarán más adelante.

Cada bloque del sistema se conforma principalmente de tres componentes: Datos (en la mayoría de los casos transacciones), un Hash del bloque y un Hash del bloque anterior. El hash del bloque se forma a partir de la los datos que contiene en su interior. Es por ello que, si alguien intenta modificar alguna transacción, el hash del bloque cambiaría completamente. Si esto ocurriera, el bloque siguiente en la cadena tendría un hash incorrecto de su bloque anterior, por lo que el bloque modificado quedaría invalidado. Esta medida de seguridad podría sortearse con facilidad si se re-calculan todos los hash de los bloques en base al primer bloque modificado, pero esto no es suficiente gracias a la principal característica de blockchain: se trata de un Sistema Distribuido peer-to-peer. Esto significa que el sistema está conformado de miles de usuarios que tienen una copia exacta de la cadena de bloques y todos en conjunto son los que validan mediante la resolución de un problema criptográfico. Un bloque se da por válido si más del 50% de los usuarios lo confirman. Esto quiere decir que si alguien logra cambiar la cadena de bloques alterando todos los hash, aun así, no llegaría a validar el bloque debido a que tiene que ser validado por la mayoría de los usuarios. Esto significa que mientras más usuarios tengan el sistema, más confiable y seguro es.

1. Se podría decir que el principal beneficio de blockchain es que es una forma completamente confiable de hacer transacciones importantes (como transferencias de dinero/bitcoins) sin la necesidad de un intermediario. La transacción es completamente directa y miles de usuarios verifican que dicha transacción es válida sin saber la identificación de las personas que están realizado dicha transacción

2. Algunas limitaciones tecnológicas que posee blockchain son:

- Escalabilidad limitada debido al “sistema de consenso” el cual restringe la cantidad de transacciones procesadas por segundo.
- Aunque la identidad del usuario es privada, las transacciones son públicas y pueden ser fácilmente rastreadas. Elevado consumo de energía producto del procesamiento de miles de nodos durante el proceso de validación (Bitcoin tiene un consumo de energía anual de 29.05 TW/h, representando el 0,13% del consumo energético mundial).