¿Qué es Blockchain?

What is Blockchain?

Autor 1: Michael Andrés Grisales González

*Risaralda, Pereira, Universidad Tecnológica de Pereira*

Correo-e: michaelandres.grisales@utp.edu.co

***Resumen*— Una introducción a lo que es la tecnología Blockchain actualmente y sus posibles aplicaciones a futuro.**

***Palabras clave—* Cadena de bloques, *hash*, minería, nodos compañeros*,* criptomoneda**

***Abstract*— An introduction to what Blockchain technology is now and its possible future applications.**

***Key Word* —Blockchain, hash, mining, peers, cryptocurrency.**

1. INTRODUCCIÓN

Aunque Blockchain es una tecnología con mucho potencial para ser aplicado a muchos campos de la informática, actualmente el público lo ve ligado intrínsecamente con la criptomoneda, lo que hace que se vea a veces con malos ojos, debido a la desconfianza que éstas presentan para la persona que no conoce la tecnología antes mencionada ni sus posibles aplicaciones. Por lo que, en el presente documento, daremos una breve introducción de lo que la Blockchain es y que se vea de forma diferente ante aquellos que lo ven como algo malo.

1. QUÉ ES BLOCKCHAIN

La idea detrás de la tecnología Blockchain se describió en 1991, cuando los científicos de investigación Stuart Haber y W. Scott Stornetta introdujeron una solución computacionalmente práctica para los documentos digitales con sello de tiempo para que no pudieran ser modificados o manipulados. El sistema usó una cadena de bloques con seguridad criptográfica para almacenar los documentos con sello de tiempo y en 1992 se incorporaron al diseño los árboles Merkle, lo que lo hizo más eficiente al permitir que varios documentos se reunieran en un solo bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004, cuatro años antes del inicio de Bitcoin.

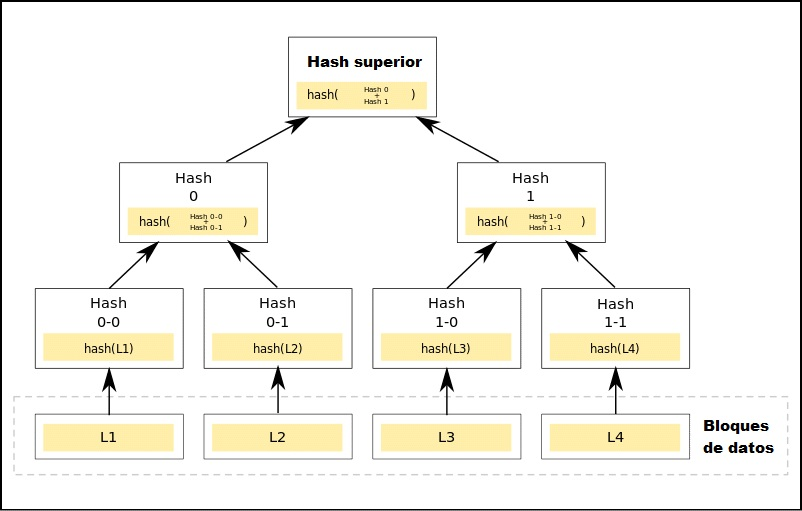


Figura 1. Representación del árbol de Merkle

1. CÓMO FUNCIONA BLOCKCHAIN

Se podría decir que básicamente Blockchain es una base de datos descentralizada y pública en la que se guardan conjuntos de transacciones en algo llamado bloques, cada bloque tiene sus respectivas transacciones y dos códigos *hash*, que son el *hash* propio y el de su antecesor (A excepción del primer bloque, llamado génesis, que solo tiene uno). Al ser descentralizada, son muchos nodos dentro de la red de *peers,* cada uno de los nodos de la red tiene una copia de las transacciones realizadas y se aplica el minado (se explicará más adelante) para que se agreguen las transacciones a su respectivo bloque. No podemos olvidar los procesos de cifrado que hay de por medio, cada transacción es cifrada con una clave pública que todos pueden ver y una clave privada que solo conoce el emisor y el receptor, lo que asegura que no haya un tercero que intervenga en la transacción.

1. MINADO

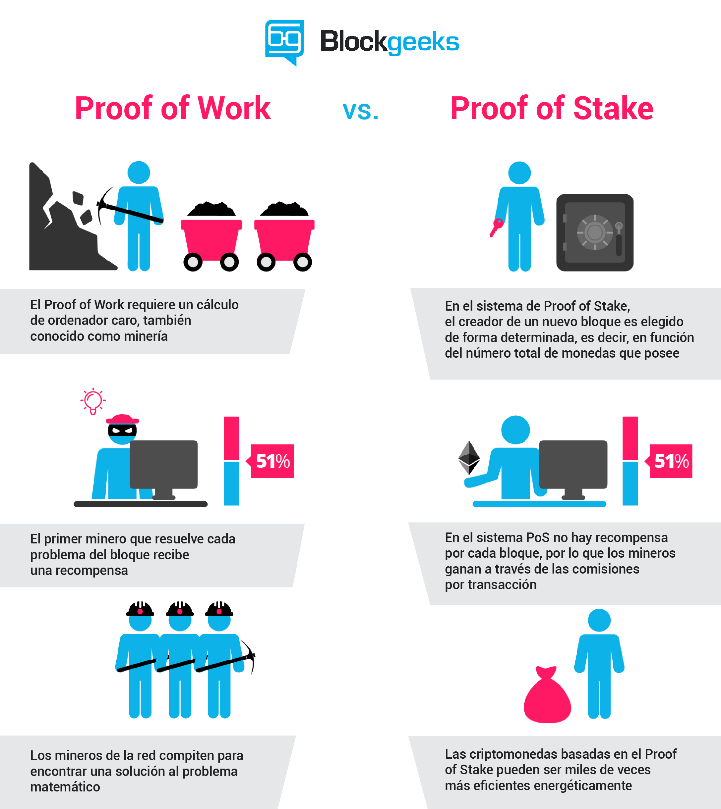
Se conoce como minería al proceso por el cual se recompensa a aquellos usuarios que forman parte de la red corriendo el software necesario y que validan y determinan el orden de las transacciones ocurridas desde el último bloque minado, para minar se usan los algoritmos de consenso.

El uso de uno u otro depende del diseñador de la Blockchain, hay 3 algoritmos de consenso actualmente utilizados:

Prueba de trabajo: PoW, del inglés Proof of Work, es un algoritmo de consenso que se basa en darle la recompensa a aquel minero que complete un acertijo matemático que significa el cierre del siguiente bloque de la cadena. Este acertijo consiste en encontrar un valor numérico, llamado *nonce,* que sirve para hacer que el *hash* del bloque con sus respectivas transacciones e incluido el *nonce*, tenga una cantidad de ceros dictada por los diseñadores de la Blockchain. Debido a la naturaleza de la función *hash*, no es posible calcular el valor de *nonce*, por lo que se debe utilizar fuerza bruta y probar con muchos valores diferentes hasta hallar el correcto. En las Blockchain con este algoritmo de consenso, mientras mayor sea el poder computacional de un nodo, más recompensas obtendrá por resolver problemas.

Prueba de participación: En inglés es conocida como Proof of Stake, de ahí las siglas PoS. Este se basa en darle la recompensa al nodo que tenga mayor cantidad de participación al momento del minado, dado que esto lo hace confiable ante los demás nodos. Debido a que es un poco injusto con los nodos más nuevos en la Blockchain, se realiza un proceso de combinación de las participaciones para elegir al quien decide el próximo bloque.

Prueba de importancia: PoI, del inglés Proof of Importance, es muy similar a la PoS, pero aquí no se aumenta la importancia gradualmente, sino que es estática a lo largo del tiempo, al momento de ingresar un nuevo nodo a la red, se le asigna una importancia, es en base a esa importancia que la red decide quién recibe la recompensa por el minado.



1. APLICACIONES

Lo que hace tan llamativa esta tecnología es el hecho de que es muy difícil de alterar un bloque ya firmado e incluso es difícil alterar transacciones aún por confirmar, para lo que se necesitaría mucho poder computacional que generalmente no suele encontrarse funcionando en conjunto, es por eso que es una de sus aplicaciones principales es la seguridad informática para guardar todo tipo de información. Eso hace que tenga aplicaciones tales como:

* Historiales médicos
* Bancos
* Contratos inteligentes
* Internet of things
* Criptomonedas
* Votaciones electrónicas

1. CONCLUSIONES

Con lo visto anteriormente, se puede decir que la Blockchain es una tecnología con mucho campo de aplicación, por lo que el hecho de ligarlo únicamente a las criptomonedas solo le quita mérito al potencial que presenta.

REFERENCIAS

Las fuentes bibliográficas deben ser citadas a lo largo del texto, deberán aparecer entre corchetes y con números arábigos. Ejemplo: Como se menciona en [1], las políticas Referencias de publicaciones periódicas:

1. Navarro, B. Y. (2017). Blockchain y sus aplicaciones. Universidad Católica Nuestra Señora de La Asunción.E. H. Miller, "A note on reflector arrays," *IEEE Trans. Antennas Propagat.*, to be published.

Retamal, C. D., Roig, J. B., & Tapia, J. L. M. (2017). La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. Economía industrial, (405), 33-40.

Referencias de libros:

1. E. Clarke, *Circuit Analysis of AC Power Systems*, vol. I. New York: Wiley, 1950, p. 81.
2. Palma, E. B. (2017). Blockchain, auditoría pública y confianza: un triángulo no. World..
3. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.
4. FRANÇA, D. (2014). BLOCKCHAIN.