BLOCKCHAIN

¿Cuando surge?

- 1991 - “How to Time-Stamp a Digital Document”
  Redactado por Stuart Haber y Scott Stornetta

- 2008 – “A Peer-to-Peer Electronic Cash System”
  Redactado por Satoshi Nakamoto

¿Qué es un bloque?

Un bloque es un registro el cual contiene datos en su interior. A dicho bloque, le vamos a añadir el hash, del bloque anterior.

¿Qué es un bloque?

Bloque

Génesis

Bloque

Dos

Datos: "Proyecto 2º ASIR"

Hash Previo: 0000000000000000000000000000000000000000000000000000000000000000

Hash Actual: 8a5059f05f5f85f8f094269be985dc251488de1c1522069701c6206d88ca57a4

Datos: "Información del bloque"

Hash Previo: 8a5059f05f5f85f8f094269be985dc251488de1c1522069701c6206d88ca57a4

Hash Actual: baaabb83e9d4b4bbee079ffb49c2542d7887c111274406413b9c831ed107b1b9

Hash

Un hash es un número hexadecimal de 64 dígitos con el cuál podemos identificar cualquier objeto digital.

Hash

Propiedades Función de Hash:

- Cualquier objeto como parámetro
- Determinista
- Unidireccional
- Efecto Avalancha
- Velocidad de Cómputo
- Soporte de colisiones

Descentralización

Blockchain es un tipo de libro mayor segurizado mediante la criptografía y el enlace de los bloques al poseer información del bloque inminentemente anterior.

Ledger

Los ledgers que podemos encontrarnos pueden ser de dos tipos:

- Ledgers centralizados

- Ledgers distribuidos

Redes P2P

La idea básica de una red P2P es que muchos nodos se conecten entre sí y reserven sus recursos para formar un sistema de distribución de contenido.

Redes P2P

Dentro de las redes P2P nos podemos encontrar con distintos tipos:

- Redes descentralizadas y estructuradas.

- Redes descentralizadas y no estructuradas.

Protocolos de Consenso

Los protocolos de consenso los cuales tienen como objetivo mantener en un correcto estado a la cadena de bloques.

- Prueba de trabajo

- Prueba de participación

El Minado

El nonce, cuyo nombre es proveniente de ‘number that can be only used once’ (número que solo puede usarse una vez), es simplemente un número. Un número aleatorio y de características únicas que tiene como finalidad ser usado en sistemas criptográficos.

Rango del Nonce

El valor del nonce no es infinito, es un número de 32 bits sin signo. Esto nos da lugar a que el número mínimo que puede tomar el nonce es 0 y el máximo es 4294967295, algo más de cuatro mil millones.

Ataque del 51%

El ataque del 51% es una vulnerabilidad teórica debido a que hoy día no se ha logrado realizar con éxito en ninguno de los grandes protocolos.

Smarts Contracts

Los contratos inteligentes son simplemente programas almacenados en una cadena de bloques que se ejecutan cuando se cumplen unas condiciones predeterminadas.