Mecanismos de consenso BLOCKCHAIN

Índice

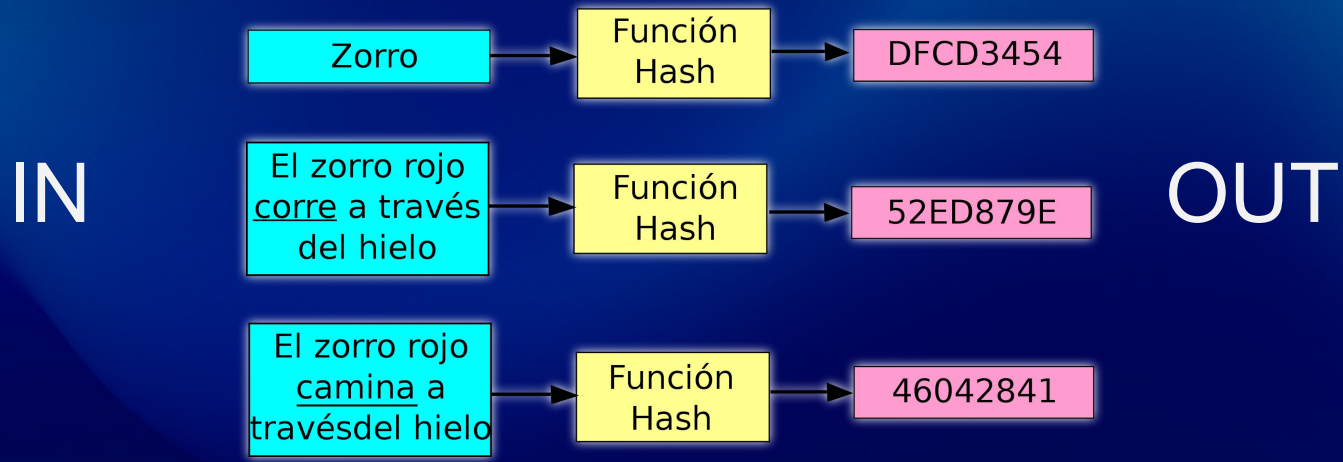
Proof of Work (PoW)

- Mecanismo de consenso descentralizado.
- Un bloque es un grupo de transacciones.
- Para añadir un bloque hay que gastar tiempo y energía en resolver un problema matemático.
- Mineros reciben recompensa por añadir bloques a la cadena .
- **Halving**: evento en el cual se reduce a la mitad el valor de la recompensa (cada 210.000 bloques añadidos en Bitcoin)
- Evita la manipulación del sistema.

Proof of Work (PoW)

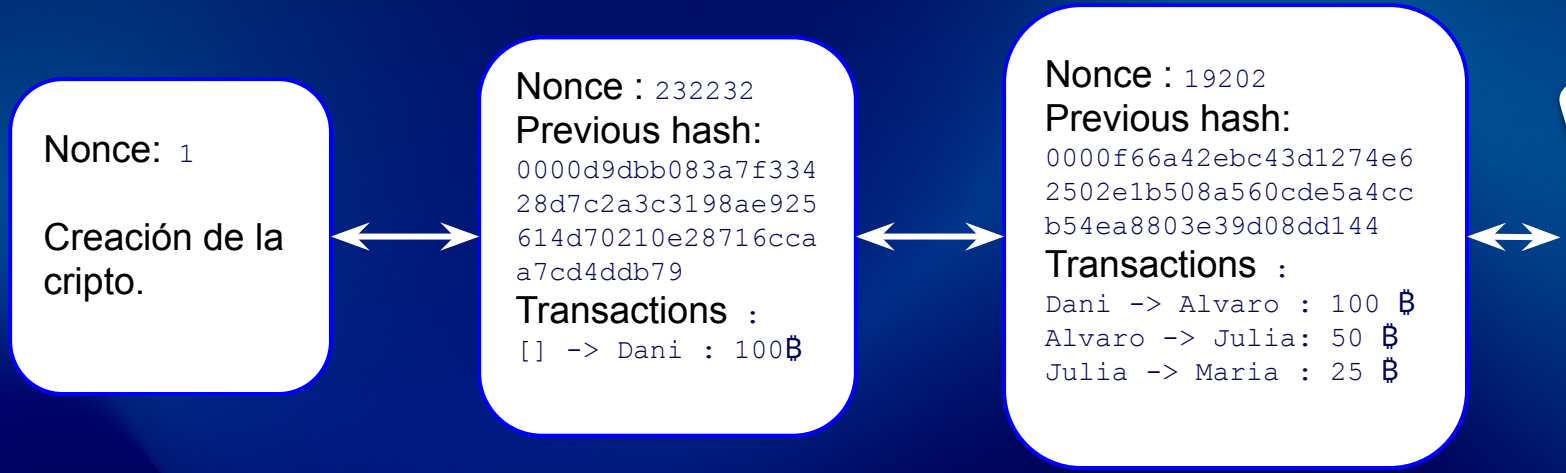
ALGORITMO DE HASH

Función resumen



Determinista, sin colisiones, unidireccional, dispersión, eficiente y tamaño fijo de salida.

Proof of Work (PoW)



Hash empiece por 4 ceros.
Algoritmo de hash : SHA-256 nonce : *'number that can be only used once '* code_link

Proof of Work (PoW)

MINADO EN BITCOIN

- 2 MB de datos por bloque y más de 800.000 bloques (434 GB).
- El hash del bloque empieza por 19 ceros.
- 10 minutos para minar un bloque.
- Se mina por pools de mineros (compartición de recursos).
- Hardware dedicado al minado (sistemas empotrados, ASIC).
- Cuantos más mineros -> más consumo de energía.
- 6,25 bitcoins / bloque minado ≈ 130.000 euros (23/10/2022).
  No es rentable (luz muy cara) ⚠️
- WEB BITCOIN.

Proof of Stake (PoS)

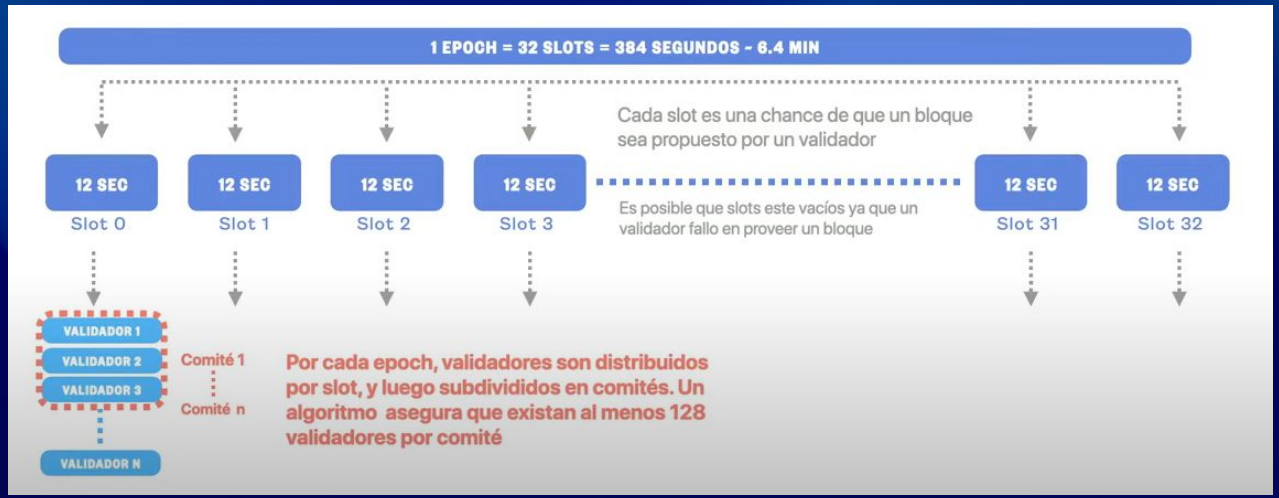
- Los nodos validadores “bloquean” una cantidad de su dinero.
  - En Ethereum, mín. 32 ETH. (43.267€ a 24/10/22)
  - Pools de Staking.
- El sistema elige a un nodo que se encarga de validar un nuevo bloque y añadirlo a la cadena de bloques.
  - Criterios de selección: cantidad, tiempo y aleatoriedad, entre otros.
- Una vez validado el bloque, el validador recibe una recompensa.
  - Nuevas monedas + comisiones de transacciones.

Proof of Stake (PoS)
¿Cómo se valida?

- El proceso de validación es diferente en cada blockchain.
- No existe nonce, se genera un hash a partir de los datos del anterior bloque y del propio dinero bloqueado (en stake).

Proof of Stake (PoS)

- Protocolo en Ethereum.
- 1 época = 32 ranuras
- 1 ranura = 1 validador + n comités
- El validador propone un bloque y un comité de validadores vota.



Proof of Stake (PoS) Penalizaciones

- Si un validador actúa de forma maliciosa es penalizado quitándole parte de su dinero en stake.
    - Ej. Si se valida un bloque no válido

FIN

Muchas gracias!

Realizado por Daniel López Marqués Y Álvaro García Barragán