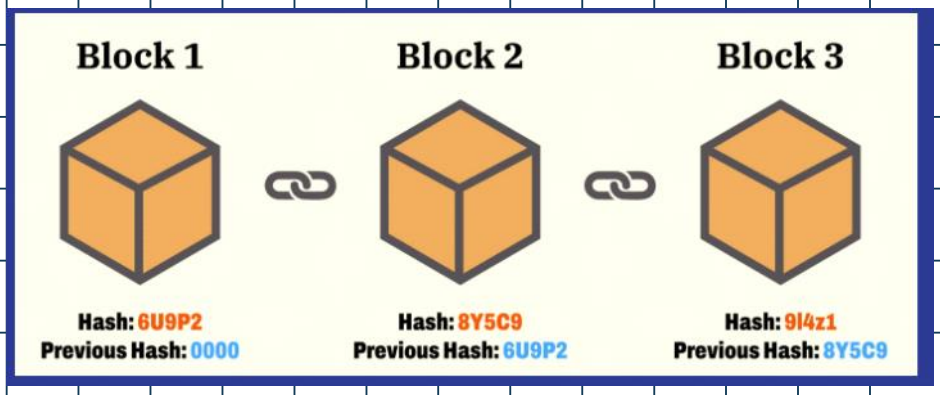
Clase 1-intro

martes, 10 de septiembre de 2024 18:40



Si yo altero un bloque ya enlazado tengo que modificar todos los bloques que le sigen porque el hash está generado con la metadata del mismo

Un bloque contiene la siguiente información:

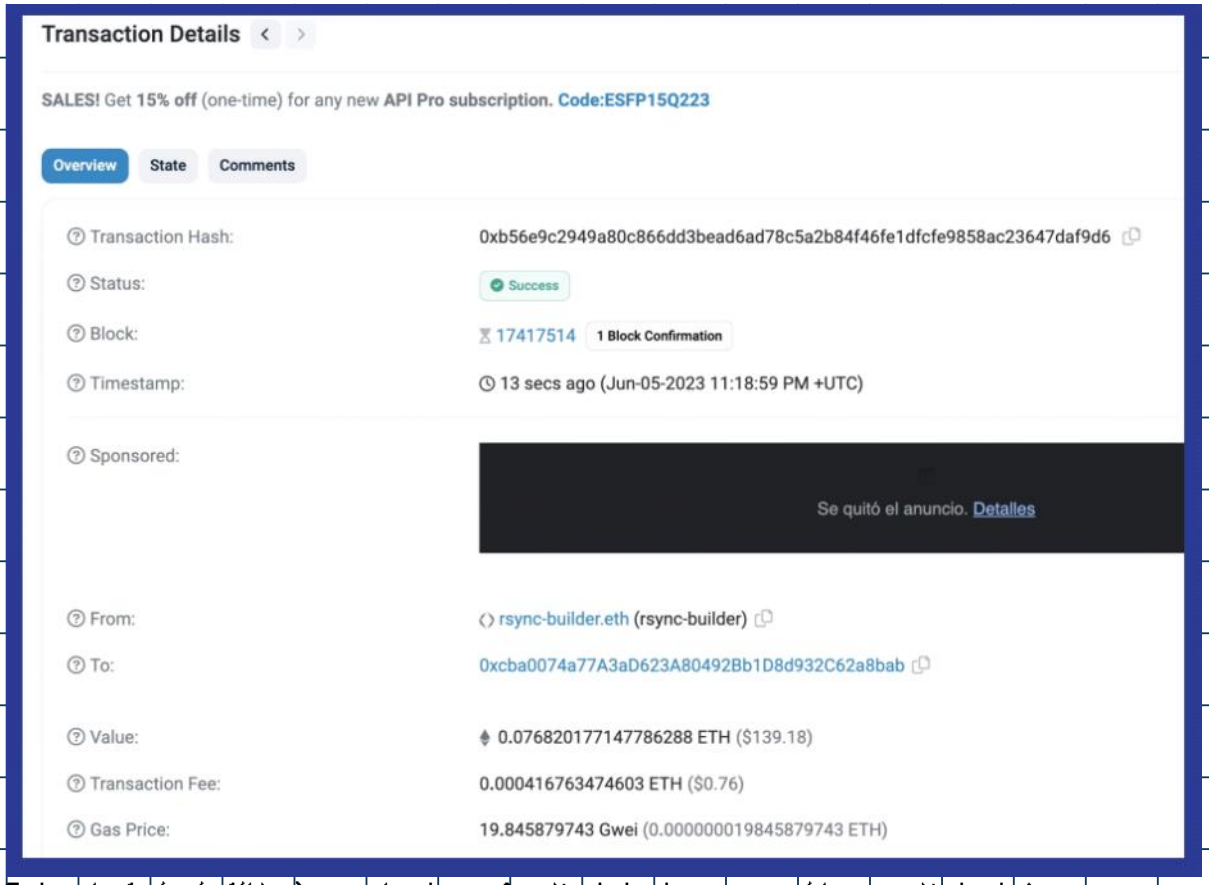
- Un hash que lo identifica.
- Una marca de tiempo.
- Referencia del bloque anterior.
- Transacciones del bloque.

Bloques tienen transacciones

Una transacción contiene la siguiente información:

- Un hash que la identifica.
- El bloque al que pertenece.
- Un remitente.
- Un receptor.
- Valor enviado.
- Una marca de tiempo.
- Está firmada criptográficamente.

El remitente firma las transacciones. Todo lo que hagamos en blockchain son transacciones



Todo esto (salvo lo último) son entradas en función de hash y genera el transacción hash. Las transacciones también son bloques (creo)

Nodo es un dispositivo, tiene toda o una parte de la cadena y se ocupa de mantener la integridad de la red.

Cada nodo tiene algo de la cadena. Entre ellos se comunican para sincronizarse. Es **descentralizado**. Si se cae uno no se cae todo. Es difícil censurar pq todos deberían ponerse de acuerdo para bajar una clave pública o algo así.

Ciclo de vida de transacción:

- Creo la metadata y la firmo criptográficamente
- Me conecto a un nodo y la propago a la red
- Pasa a espera (mempool).
- Un validador o minero agarra mi transacción y la mete a un bloque para meterla a la red
- Se confirma la transacción

Validar: los nodos de la red hacen cositas para ver que esté todo bien. Todos tienen que aceptarlo y tener la copia del nuevo bloque que meti

Cuando uno mina lo que hace es crear bloques que cumplan con ciertas reglas y subirlo a la red
Bitcoin usa proof of work para validar que sea correcto
Transaction fee: comisión va a quien valida o mina una transacción
Minar un bloque es armar un bloque y que forme parte de la red.
Nodos compiten para tratar de resolver un desafío criptográfico. Tomo una transacción, genero un hash que tiene que tener una cantidad delantera de 0 para que sea válido (tengo que ir haciendo prueba y error hasta que consigo un hash que cumple mi regla). Una vez que lo consigo los otros nodos validan que lo que hice esté bien. A mayor cantidad de 0s más dificultad
La dificultad aumenta a más mineros hay. Cada 10 minutos hay un nuevo bloque

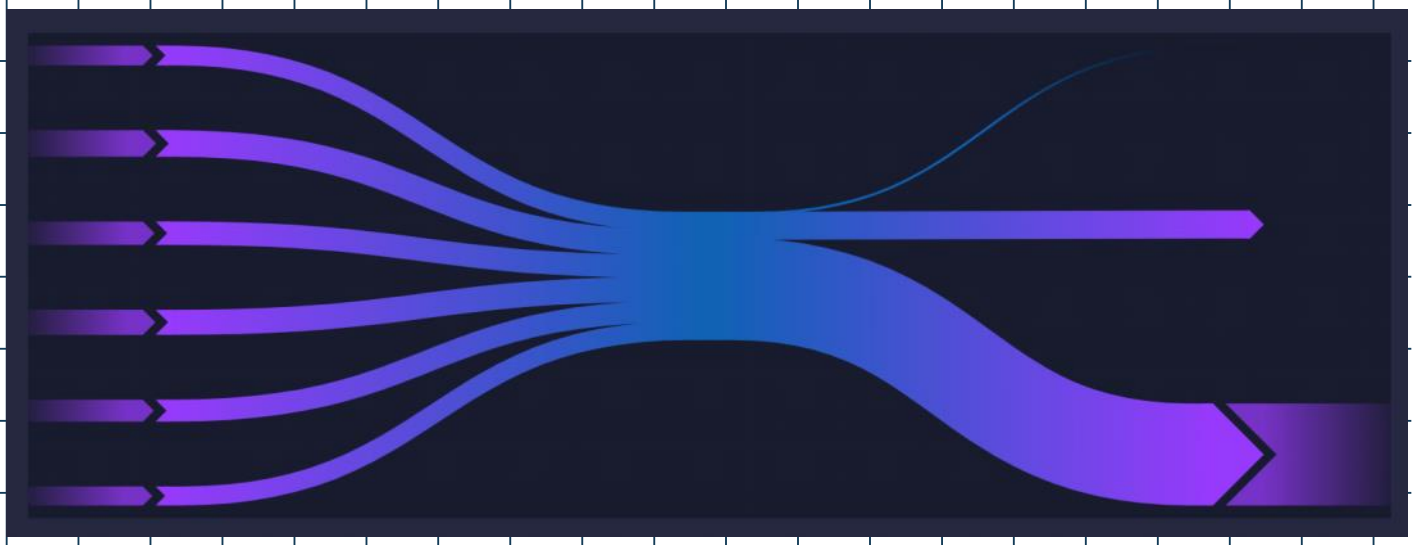
Si se generan dos bloques en simultáneo, las van a mandar a bloques cercanos. El próximo que intente mandar un nuevo bloque va a hacerlo y va a tener uno de los dos bloques. Entonces el que primero que se suba queda básicamente pq siempre queda la cadena más larga

Transacciones UTXO

Cuando mandamos bitcoin se usan las salidas no gastadas de transacciones anteriores.
Cada transaccion tiene 2 salidas.

- Una interna: yo tengo 2b, tansfiero 1 y el otro que me queda no vuelve a donde estaba antes sino a una nueva dirección.
- Externa: a quien le estoy haciendo la transacción.

Esto ayuda a que sea más seguro



Frase semilla
De 12 a 24 paalbras que de manera determinística genera claves privadas y públicas