Breve historia de Bitcoin. Transacciones, bloques, hashes y recompensas

4 octubre, 2021

Bitcoin es un conjunto de tecnologías, así como el nombre de la moneda, basados en la tecnología blockchain. Bitcoin se basa en un libro de cuentas distribuido entre múltiples nodos repartidos por Internet, en forma de una cadena de bloques llamada Blockchain .Los nodos comparten información y crean bloques, manteniendo toda la estructura de bitcoin.

Los bitcoin

- La moneda se llama bitcoin. Existen unidades más pequeñas que un bitcoin
- Las monedas se van creando poco a poco. Cada vez que se crea un bloque se generan bitcoin
- Actualmente cada 10 minutos se crean 6.25 bitcoin, que se ingresan en la cuenta del minero que crea el bloque correcto
- En 2140 se estima que se habrán creado todos los bitcoin
- El máximo de monedas que habrá serán 21.000.000 de bitcoin. Ni más ni menos.
- Un satoshi es equivalente a 0.00000001 bitcoins
- Podemos comprar bitcoin con nuestro dinero, y venderlo a cambio de dinero.
- La cantidad de euros a que equivale el bitcoin cambia con el tiempo.
- Los bitcoin no existen, solo existen como anotaciones en el libro de cuentas
- Las personas que minan un bloque con éxito, se «autotransfieren» una cantidad fija de la nada
- Las cuentas
- Cada persona crea al menos una cuenta, identificada con un código
- Esta cuenta está protegida con claves criptográficas únicas, que solo tiene el dueño
- En ningún momento se asocia esta cuenta con unos datos reales
- Si se pierden las claves, se pierde el acceso a la cuenta y, por tanto, el acceso al dinero
- Estas cuentas se guardan en billeteras o wallets. Estas no contienen dinero alguno, solo las claves.
- Podemos tener claves de varias criptomonedas en una misma billetera.
- Las transacciones
- Cada cuenta tiene una dirección pública, aunque no se asocia a una persona públicamente.
- El dinero se mueve de una cuenta a otra mediante transacciones
- Las transacciones son movimientos de dinero entre varias cuentas.
- Las transacciones son públicas, y cualquiera puede verlas
- Deben ser confirmadas para que tengan efecto. Al hacer una transacción, parte del dinero pagado se descuenta para luego repartirse como recompensa (como una - comisión)

Los bloques

- Cuando se tiene un conjunto de transacciones, se crea con ellas un bloque con ellas
- Los mineros compiten por crear un bloque válido.
- Cada diez minutos de media se crea un bloque válido
- Una vez se crea un bloque válido, se agrega a la cadena de bloques existente.
- El 3 de enero de 2009 se crea el primer bloque.

- Los bloques tienen un número que los identifica. El bloque original es el bloque 0.
- En este bloque, la primera transacción es una cantidad de bitcoins creados nuevos a su cuenta
- Si su bloque sale adelante, las transferencias de dentro se confirman, y se lleva la recompensa.
- Las recompensas van disminuyendo cada 4 años (50,25, 12.5, 6.25, etc).
- A día de hoy (octubre de 2021) existen alrededor de 700.000 bloques creados

La cadena blockchain

- Los bloques se apilan uno encima del otro, formando una pila.
- Cada bloque que se apila está formado a partir del anterior, con parte de su información
- Esta cadena de bloques se llama blockchain
- Toda esta información, que ocupa actualmente 400 GB, se guarda en múltiples ordenadores
- Estos ordenadores se llaman nodos, y se van intercambiando la información
- Bitcoin existe mientras todos estos nodos guardan copias de la información
- Las recompensas
- El sistema se sostiene gracias a recompensas. Las transacciones y los bloques dan recompensas.
- Los mineros dedican potencia de ordenadores a crear bloques, a cambio de la posibilidad de ganar dinero
- Para este minado se necesita cada vez más potencia de computación

Los hashes

- El sistema intenta que los bloques se vayan creando regularmente cada 10 minutos de media
- Para ello, pone un reto de dificultad que tarde un tiempo en poder resolverse
- Este reto consiste en crear un código utilizando criptografía llamado hash
- Este hash se genera a partir de información del bloque actual, y del anterior
- Cada hash identifica un bloque, y se calcula con el hash del bloque anterior.
- Crear un código hash requiere muy poco tiempo
- Para complicar la tarea, se pone una condición que el hash debe cumplir
- Se tienen que hacer muchas pruebas hasta allar un hash válido
- Este cálculo es más rápido a medida que la potencia de los ordenadores aumenta
- Por ello, la dificultad se va ajustando poniendo una condición más estricta
- El nonce es el parámetro que hay que variar hasta conseguir un hash válido.