Conceptos Esenciales

- Confianza
- Transacciones
- Problema del doble gasto
- libro contable
- intermediarios
- problema del general bizantino.
- Dificultad de red: esfuerzo computacional para crear un nuevo bloque.

En 2013 sucedió el primer fork producido por un desacuerdo entre los miembros de bitcoin.

- Hard Fork: Cambio del protocolo que resulta en dos ramas: se crea una versión duplicada y una nueva criptomoneda. Aparece una nueva criptomoneda y la vieja sigue estando disponible, pudiendo vivir en paralelo.
- Soft Fork: Actualización del protocolo.

Forks importantes:

- Bitcoin cash (BCH)
- Bitcoin Gold (BTG)
- Bitcoin Private(BTCP)

Efemérides

MT.Gox

- Primer cryptoexchange que operó entre 2010 y 2014, manejando el 70% de las transacciones de bitcoin.
- De repente suspendieron actividades y declararon bancarrota
- Se perdieron 450 millones de dolares (850btc)

En 2021 el canto suizo de Zug fue el primer lugar en aceptar bitcoin para pagar impuestos, también se acepta en el salvador bitcoin como moneda de curso legal.

BlockChain

Es un registro, como un libro de contabilidad público que solo puede ser actualizado por consenso de la mayoría de los usuarios del sistema. Solución de código abierto. Una blockchain NO es para almacenar datos, se debe minimizar lo que se almacena en ella.

Subsistemas e infraestructura

- Nodos validadores: verifican transacciones y aprueban modificaciones de acuerdo al protocolo de consenso
- Nodos ligeros

- Redes de acceso
- dispositivos clientes
- Centros de cálculo
- red central
- Almacenamiento distribuido: almacenan el ledger.

Tipos de blockchain

- Permisionada: participantes conocidos, No Proof of Work (no minado), no hay necesidad de criptomoneda, tecnología de BBDD distribuida
- No Permisionada: Participantes desconocidos, Proof of Work, Criptomoneda nativa, Crypto Economics.

Métricas de evaluación

- Rendimiento: Número de transacciones exitosas por segundo
- Latencia: Tiempo que demora realizar una transacción
- Escalabilidad

Diferencia bitcoin y ethereum

- Orientado a transacciones vs orientado a smartcontracts

Tipos de cuenta ethereum

- Titularidad externa: como las de bitcoin
- Cuenta de contrato: para los smart contracts

Contrato inteligente

- Ni es inteligente ni es legal
- Complicados de cambiar
- Tarifa por Gas: coste por transacción, computa las necesidades de código. Se utiliza para pagar el esfuerzo de los mineros. Cada bloque tiene un máximo de gas
- Tarifa de prioridad

Los contratos pueden tener varias aplicaciones:

- Certificados académicos
- Seguimientos de procedencia y trazabilidad

Consenso

- Forma de llegar a un acuerdo
- Evalua la capacidad de la red para que nodos independientes lleguen a un consenso sibre una

única versión de la vedad
- Esencial para permitir las transacciones en los sistemas blockchain

Trilema de blockchain

- Escalabilidad de la red: Transacciones por segundo
- Descentralización: Número de nodos que participan
- Seguridad: Cantidad de recursos necesarios para corromper el consenso.

Proof of Work

- Protocolo de consenso de blockchain publicas
- Competición criptográfica de resolución de puzzles entre nodos validadores o mineros establece el consenso.

Resolver el puzzle consiste en determinar un rango de entrada que da como resultado un objetivo predefinido

- El nonce es la entrada desconocida que los mineros compiten por encontrar

La escalabilidad de bitcoin se limita a validadr 1MB de datos de transaccion cada 10 minutos.

Proof of Stake

En lugar de utilizar capacidad computacional se basa en la cantidad de tokens que tiene un usuario. Se habla de bloques forjados en vez de minados. Para encontrar el validador de la red se usa una lotería. Los validadores se seleccionan en función a la cantidad de tokens. Favorece a los nodos con mayor número de tokens.

Delegated Proof of Stake: Se eligen delegados responsables

POW vs POS

POS es mas centralizado pero más eficiente energéticamente POS es menos seguro que POW

Proof of Authority

Hay un listado de autoridades preseleccionadas que tienen el poder de validar los bloques, son autoridades conocidas y confiables, lo que permite una mayoer ficiencia y escalabilidad. Los nodos deben actual honorablemente para proteger su reputación. Rápida eficiente y muy escalable.

Byzantine Fault Tolerant

A prueba del problema de la falla bizantina, a prueba de que algun nodo no reaccione de forma honesta. Se usa en blockchain empresariales y de consorcio. Los nodos se ponen de acuerdo en un

lider y requieren una mayoría para validar las transacciones. Usa formato round robin para modificar el nodo líder. Puede tolerar un tercio de nodos defectuosos o deshonesto. Es más rápido que POW, además es más barato y eficiente energéticamente.

Proof of Burn

Sistema POW sin derroche de consumo energético:

- Los interesados envían cierta cantidad de criptomoneda a una dirección conocida como dirección de quemado o consenso.
- Estas se consideran quemadas y eliminadas del suministro, no se deberían poder gastar.

Proof of elapsed time

Desarrollada por intel. Para redes permisionadas, se basa en sistemas de loteria, distribuye de forma equitativa las posibilidades de ganar, da la misma posibilidad a todos los nodos. El nodo que tenga el tiempo de espera más corto es el que gana. Consume menos energía ya que los nodos estan en sleep.

Proof of History

Propuesto por Solana como lockchain de alto rendimiento. Proporciona una secuencia de eventos ordenados de manera confiable y verificable. Mayor latencia en transacciones.

Proof of importance

Propuesto por NEM. Busca que los participantes estén comprometidos, la importancia va en función a la actividad realizada, saldo alto, transacciones, etc… en función de esta importancia se establece la probabilidad de crear nuevos bloques o procesar transacciones.

Proof of activity

Combinación de POW y POS. Cuando se mina un bloque la funcionalidad cambia a POS. Hay un grupo de validadores seleccionados de forma aleatoria. La recompensa se reparte entre el minero y el validador. Criticado por no solucionar ningún problema de POW y POS.

Proof of Capacity

Se centra en la capacidad de almacenamiento de los participantes. Se genera una lista de hashes llamada ploting. Aprovecha que el almacenamiento es más accesible y eficiente. El problema es que tiende a la centralización.

Proof of space

Se centra en demostrar la asignación y uso eficiente del espacio de almacenamiento.

Proof of weight

Mide la antiguedad de las criptomonedas y la participación en la red

Proof of identity

Se basa en la identidad de los participantes. La identidad debe estar verificada y en función a ella se participa en la validación de las transacciones. La verificación de la identidad se hace fuera de la blockchain

Prueba de reputación

Los nodos ganan influencia y derecho de participación en función de su reputación.

Proof of location

Se centra en la ubicación geográfica de los nodos

Credit based POW

Combina pow con pos. Se pueden comprar créditos para tener mayor probabilidad de ser el nodo seleccionado para un bloque. Trata de buscar el equilibrio entre Pow y Pos, tratando de reducir el uso computacional.

Ataques a protocolo de consenso

- Ataque del 51%: Ocurre cuando un solo actor controla más del 51% de los nodos, le da el control para manipular la blockchain.
- Ataque Sybil: Un atacante crea multiples nodos para obtener
- Ataques de desconexión
- Ataques de rollback: tratan de revertir las transacciones
- Ataques de ataque Grinding: Se enfoca en intentar manipular el proceso de selección del validaddor
- Validador malicioso.