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

From:
http://www.knoppia.net/ - **Knoppia**

Permanent link:
http://www.knoppia.net/doku.php?id=bc:cesenciales

Last update: **2024/10/07 16:38**