Skycoin

1 Skycoin

Skycoin es todo un ecosistema donde la cryptomoneda es solo una parte de la historia. El resto incluye la eliminación de los premios de minado, desarrolla un Hardware eficiente desde el punto de vista de Energético, la realización de transacciones veloces y la promesa de una segura y privada alternativa a Internet.

2 Mayores componentes del ecosistema de Skycoin

- Skycoin: Rápida y segura moneda respaldada por ancho de banda.
- Skywire: Anónimo y descentralizado mesh-Intenet.
- Skyminer:Hardware y punto de acceso para Skywire.
- Fiber: Red Blockchain Descentralizada.
- Skysuite: Conjunto de Aplicaciones descentralizadas.

3 Principales características de Skycoin

El Proyecto Skycoin es uno de los más viejos en desarrollo, y Skycoin es la primera de sus creaciones. Construido sobre la infraestructura centrada en la fundación de un Internet descentralizado. Skycoin corre sobre un algoritmo de consenso totalmente nuevo, `Obelisk` o como también lo conocen 'web-of-trust'. Con Obelisk Skycoin no es susceptible a las debilidades de 'Proof of Work'(Pow) y 'Proof of Stake'(PoS).

- Sorprendentemente rápido:
- Transacciones toman tan poco tiempo como 2 segundos. Sin cuellos de botella o sobrecargo, Skycoin es más rápido que otras criptomonedas y compite contra tarjetas de crédito y Apple Pay.
- Cero sobrecargo:
- Las transacciones cuestan `Coin Hours`', una moneda separada pagada por los contenedores de Skycoin por cada hora qué ese mantiene un Skycoin.
- Segura:
- Construida desde la base de Goland, Skycoin hace uso extensivo de los estándares criptográficos para asegurarse que las transacciones no son vulnerables a amenazas como ataques del 51%, reverso, duplicación y maleavilidad.
- Privada:

- La estructura de las transacciones en Skycoin fueron diseñadas para adoptar el protocolo CoinJoin. Una vez integrado, Skycoin mezcla las transacciones de múltiples wallets para asegurarse de que sea indistinguible de uno a otro.
- Sostenible:
- Sin la enorme carga computacional de los requerimientos típicos de PoW y PoS, Skycoin puede correr en un procesador de un celular de 30 watts.
- Incentivada:
- Skycoin es más que una criptomoneda. Tiene un valor agregado de la red Mesh Skywire.
- Utilidad respaldada:
- Aplicaciones prácticas de Skycoin son respaldadas por un activo: Ancho de Banda.

4 Obelisk

Obelisk, algoritmo de consenso único de Skycoin, es el centro de todo el ecosistema de Skycoin. Consenso Web-of-trust cambia la manera en que nosotros entendemos y usamos las tecnologías de blockchain. Este remueve la necesidad de costosos recursos para minar, elimina el vicioso ciclo que da el incentivo de minar, aumenta exponencialmente la velocidad de las transacciones, y entrega gran seguridad.

5 Problemas de Bitcoin y la debilidad de Proof-of-Work

En los primeros momentos de la programación de Bitcoin, existió un mal cálculo respecto a que el proceso de minado iba a provocar un incentivo económico cuya estructura conduce a la des centralización. En su lugar, PoW concentra su influencia sobre piscinas de minado que pueden proveer a recursos a los mineros con poco poder. Esos mismos grupos de influencia pueden orquestar cambios extendidos a la red.

Se identificó el control de minado como el mayor problema no-criptográfico de la red de Bitcoin, dado la posibilidad de un ataque del 51%, cuando más del 50% del poder de hashear está en manos de solo un selecto grupo.

Eso implica que las operaciones de la red son a la vez económicamente y ambientalmente ineficiente.

De acuerdo al investigador de energías `Sebastián DeetMan`(2016):

> Si la red de Bitcoin se mantiene expandiendo... puede llegar a un alto consumo de electricidad... [equivalente a] el consumo total de Denmark en 2020.

El enorme costo de minar puede ser influenciado exponencialmente por más capital y más usuarios. Como sea, pocas monedas fuera de Bitcoin y Ethereum tienen el poder de mantener tal crecimiento.

6 La tendencia a la centralización de Proof-of-Stake

Aunque el algoritmo de PoS elimina el problema del 51%, tiene incluso más vulnerables a la centralización de las redes que PoW. Con PoS, el tamaño de las tenencias de un participante en una moneda particular(o "stake") determina su poder de votar por cambios técnicos en la red. Participantes también tienen que minar una porción equivalente a su stake, independiente de su capacidad de procesamiento.

Este principio significativamente incrementa las barreras de lanzar un ataque del 51%. El costo financiero de adquirir la mayoría de los token de la red en el mercado abierto, excede la ganancia potencial. Además, si un atacante con éxito se convierte en el accionista mayoritario en la red, sufrirán la mayor parte del ataque debido al impacto en la estabilidad de la red y la respuesta del mercado.

Aunque esto sube la barrera de los ataques a la red, PoS crea un impulso centralizado igual a PoW.

7 La solución: Obelisk, Algoritmo de consenso distribuido

Para eliminar este problema, Skycoin usa un algoritmo distribuido de consenso, `Obelisk`. Obelisk distribuye la influencia sobre la red de acuerdo a `web-of-trust`. En vez de mineros, la red consiste en nodos (computadoras, Skyminers. . .) y cada nodo se suscribe a una lista de nodos de confianza. Nodos con más subscriptores tienen más influencia en la red.

Cada nodo es asignado a un blockchain personal, que actúa como un canal `público de broadcast`, donde cada acción es públicamente guardado y visible. Como todos las decisiones del consenso y las comunicaciones ocurren sobre un elblockchain personal de cada nodo, la comunidad puede fácilmente auditar nodos por engaño o corrupción -Sin comprometer la privacidad-. Los nodos son direccionados por su llave criptográfica pública y una dirección deI IP que solo se conoce por los nodos a los que esta directamente conectados.

El récord público dejado por el blockchain personal de cada nodo le permite a la red reaccionar ante la detección de otras conexiones maliciosas. Bajo el mismo principio, si la comunidad detecta que el poder de la red está demasiado concentrado (o no concentrado lo suficiente), la comunidad tiene la potestad de balancear el poder de cambiando las relaciones de confianza.

La contabilidad de los nodos para la comunidad y auditorias así como la transparencia de las decisiones tomadas en consenso, introduce un factor democrático

y descentralizado a la red.

Solución que brinda Obelisk

- Alta escalabilidad y bajos niveles de consumo de energía: -Este algoritmo de consenso fue diseñado para ser escalable y sin altos gastos computacionales, siendo una mejor alternativa a PoW. La centralización se vuelve más difícil cuando más personas tienen acceso.
- Robusta defensa contra ataques coordinados:
- Obelisk soporta un ataque a gran escala de una red bien organizada de nodos maliciosos. El algoritmo no es iterativo, converge rápido, puede correr en una red esparcida con solo conectividad con los nodos adyacentes, y funciona bien ante la presencia de ciclos en el grafo de conectividad.
- Protegiéndose contra ataques del 51%:
- Este consenso previene el desarrollo de un poder centralizado. Skycoin no se auxilia de mecanismos de minado, y no es susceptible a las vulnerabilidades de Pow/PoS.
- Direcciones de IP ocultas:
- Los nodos están conectados por su llave pública criptográfica. La dirección IP es solo conocida por los nodos directamente conectados.
- Independencia de la sincronización del reloj:
- El algoritmo no usa un reloj global. En su lugar, secuencias de numéricas de bloques que se extraen de el consenso validado y el blockchain, lo cual se usa para calcular el tiempo interno del bloque. Esto puede ser internamente llamado `reloj del bloque`.

8 Coin Hours

Las transacciones en Skycoin no incluyen sobrecargo. El sobrecargo en las transacciones, similar a los premios de los bloques que incentivan a los mineros to drive up al costo de la red, solamente creando incentivos monetarios a la con efectos adversos eliminando sobrecargo en las transacciones.

9 Skycoin CX vs Ethereum

CX	Solidity
Completo	Funcionalidad limitada

CX	Solidity
Amigable para los programadores(Basado en Golang)	Desconocido para la mayoría de los programadores
Diseñado para juegos, aplicaciones y contratos inteligentes	Solo diseñado para contratos inteligentes
Incluye motores gráficos(CXFX)	No tiene motores gráficos
Compilado e Interpretado	Compilado
Ilimitado número de transacciones por segundo	Máximo 15 transacciones por segundo
No hay sobrecargo en las transacciones	ETH cargo por las transacciones
Cada juego/aplicación tiene su propio blockchain	Todos los juegos y aplicaciones comparten el mismo blockchain