



Lideran



Expe riencia tech 2022

19 y 20 de oct.

Centro Empresarial El Poblado

Vive la **evolución digital**

Blockchain como herramienta de cambio



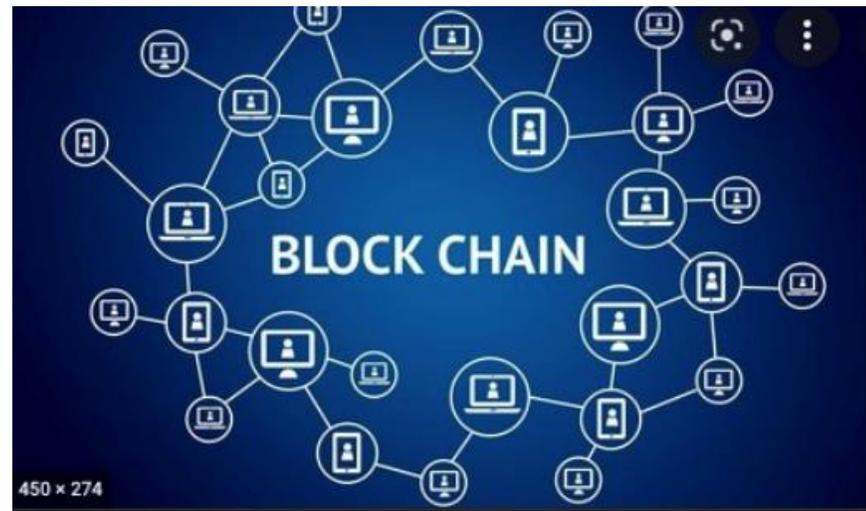
Oscar Bertron.
Blockchain Community Leader at
Hash House

Mauricio López
Gerente Comercial Hash House

¿Qué es Blockchain ?

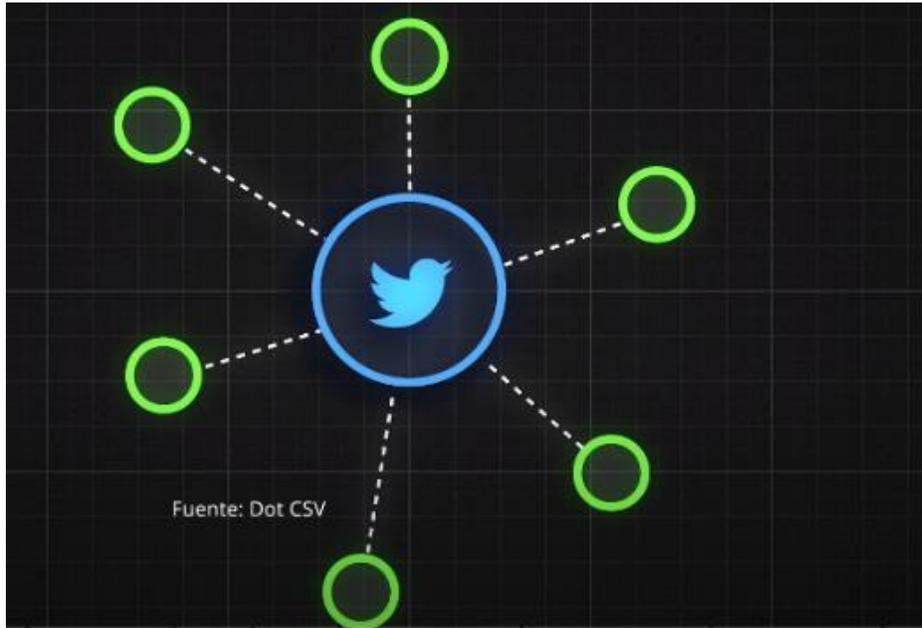


Base de datos descentralizada, administradas por nodos iguales (P2P), los cuales, a través de un sistema de consenso, clasifican, gestionan, organizan y añaden información a lo mismo, sin posibilidades de generar una alteración y sin necesidad de un organismo central de validación de datos.

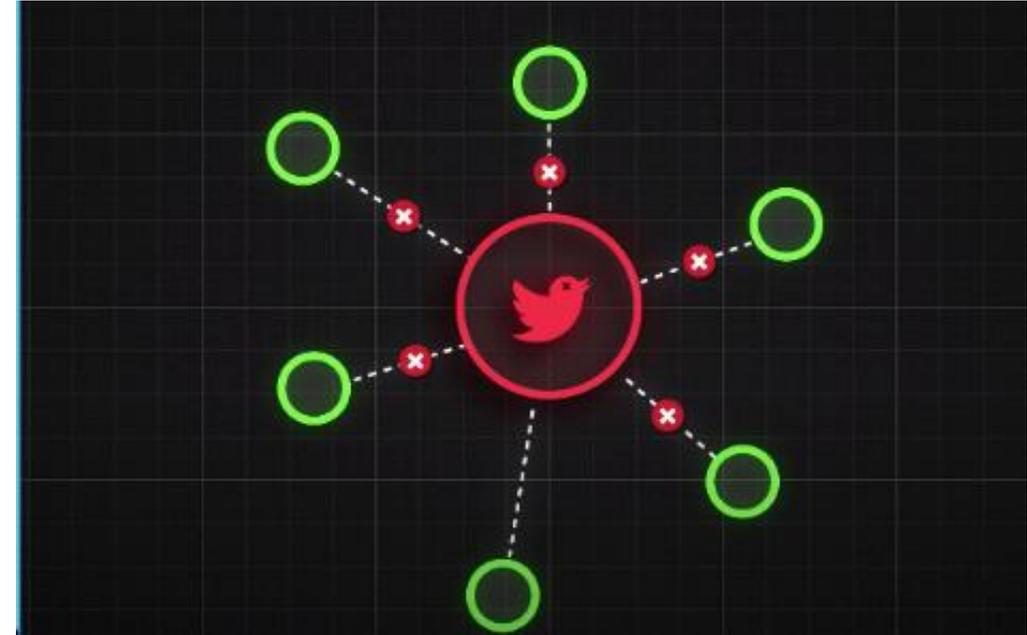


¿Por qué se crea?



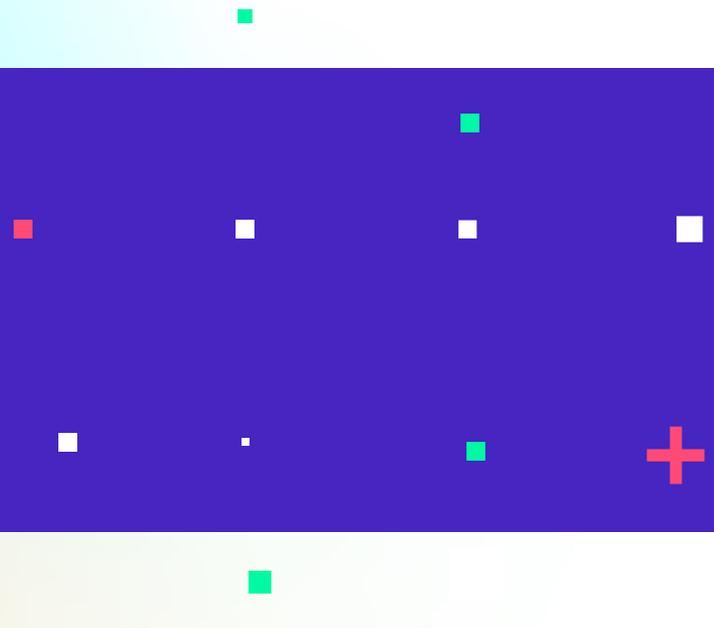


- Facilita gestión de datos
- Toma de decisiones centralizadas
- Control de datos para fines privados



- Vulnerabilidad a ataques informáticos
- Fallas en nodo central
- Centralización de poder
- Sesgos de información

Solución propuesta

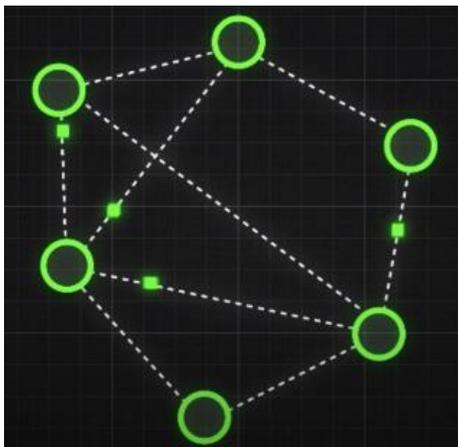


Sistema de distribución de datos P2P, en el cual, los nodos participantes llegan a un consenso sin actores centrales

¿Cómo se ponen de acuerdo los nodos?

Ejemplos previos:

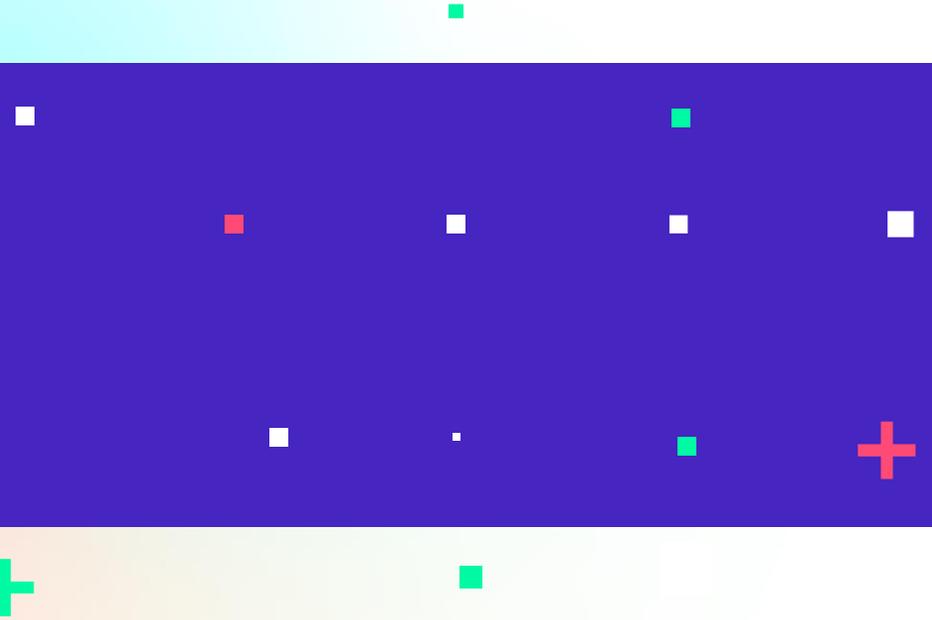
- Torrent
- Ares
- Limewire



2 Formas principales de consenso:

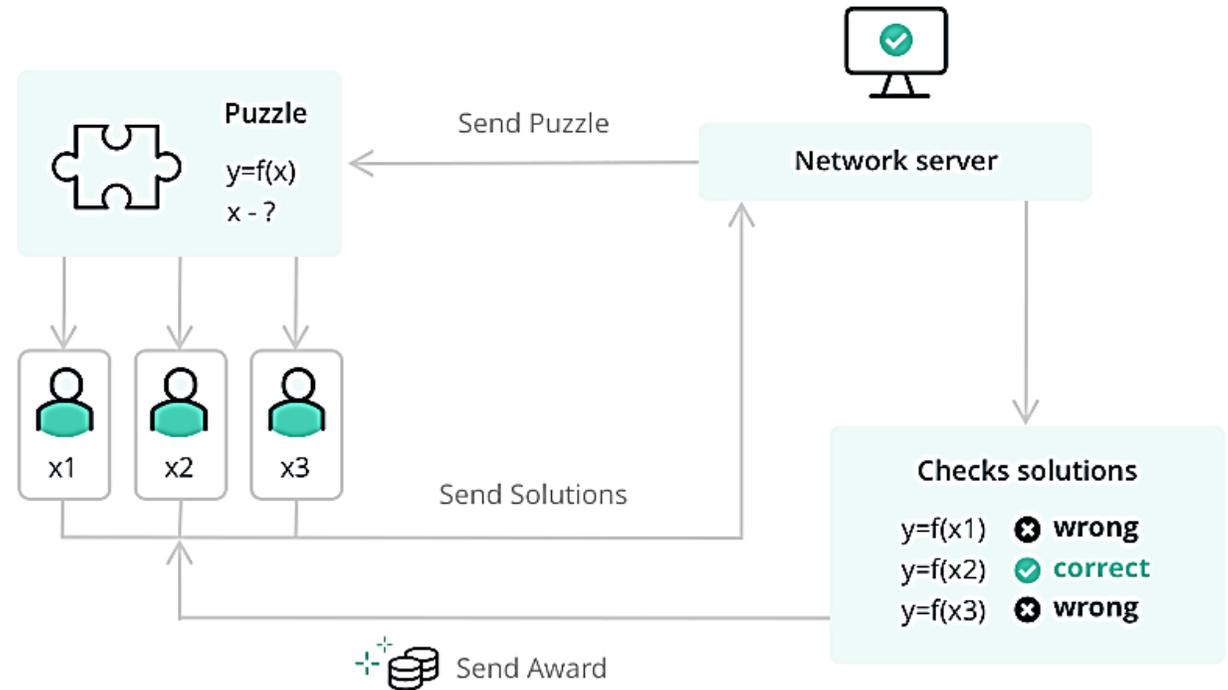
- PoW: Proof of Work
- PoS: Proof of Stake

Proof of Work



Mecanismo usado para ganarte tu participación en un proceso electoral, invirtiendo parte de tu recurso computacional.

Al ser pares que no se conocen, demostrar que se genera un gasto computacional, técnicamente, demuestra que el nodo validador es de confianza.



Fuente: ledger.com

Bitcoin

Sistema de dinero electrónico
en efectivo Peer to Peer

Satoshi Nakamoto

Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario

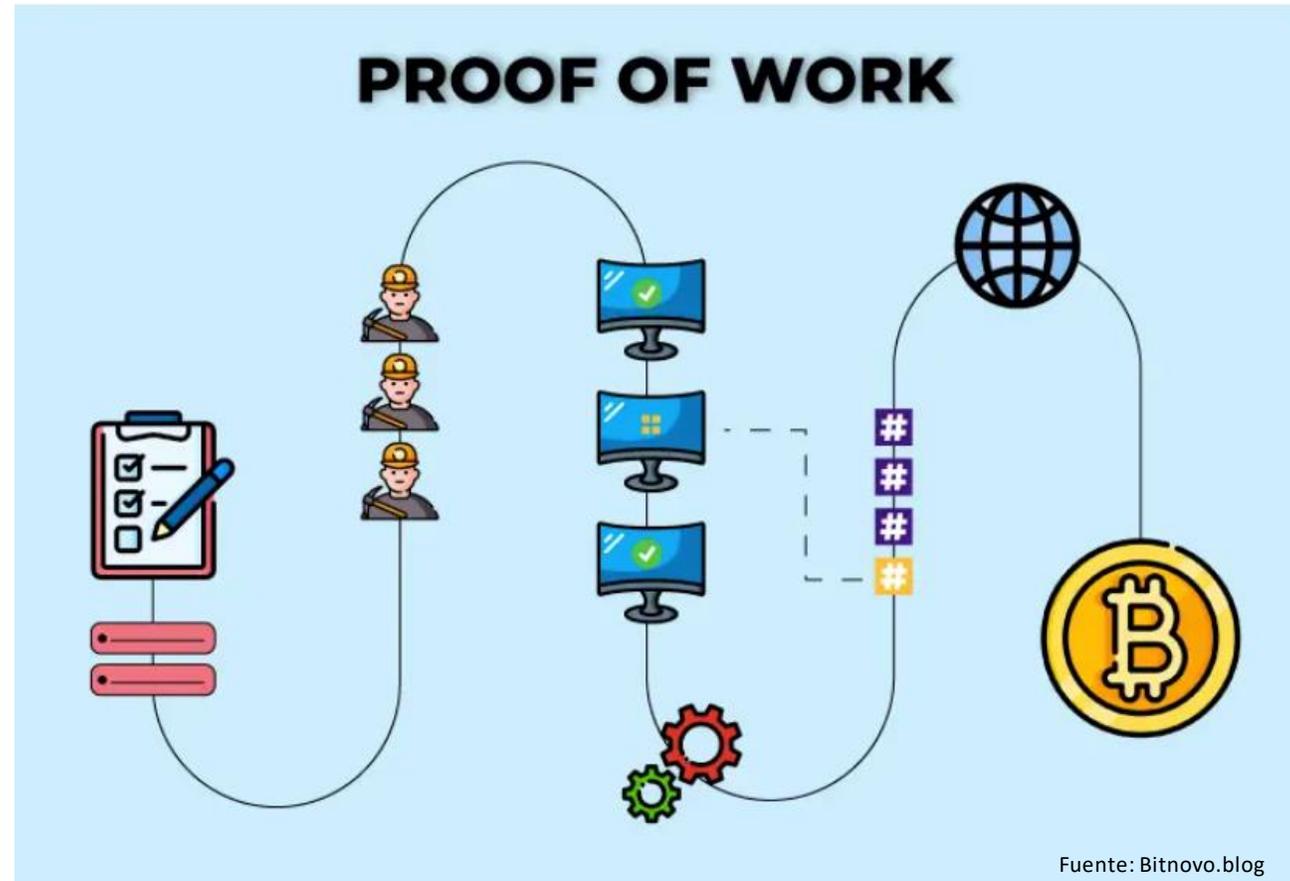
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Traducido al Español de bitcoin.org/bitcoin.pdf
por Angel León - www.diariobitcoin.com

Abstracto. Una versión puramente electrónica de efectivo permitiría que los pagos en línea fuesen enviados directamente de un ente a otro sin tener que pasar por medio de una institución financiera. Firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si existe un tercero confiable para prevenir el doble-gasto. Proponemos una solución al problema del doble gasto utilizando una red usuario-a-usuario. La red coloca estampas de tiempo a las transacciones al crear un hash de las mismas en una cadena continua de pruebas de trabajo basadas en hashes, formando un registro que no puede ser cambiado sin volver a recrear la prueba de trabajo. La cadena más larga no solo sirve como la prueba de la secuencia de los eventos testificados, sino como prueba de que vino del gremio de poder de procesamiento de CPU más grande. Siempre que la mayoría del poder de procesamiento de CPU esté bajo el control de los nodos que no cooperan para atacar la red, estos generarán la cadena más larga y le llevarán la ventaja a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia.

Libro contable (Ledger) en el cual se registran todas las transacciones que se hacen entre usuarios. Los nodos se encargan de verificar las transacciones mientras están en una competencia por resolver un problema matemático de alta complejidad

Las transacciones se registran en BLOQUES de información, validado y almacenado por la red.



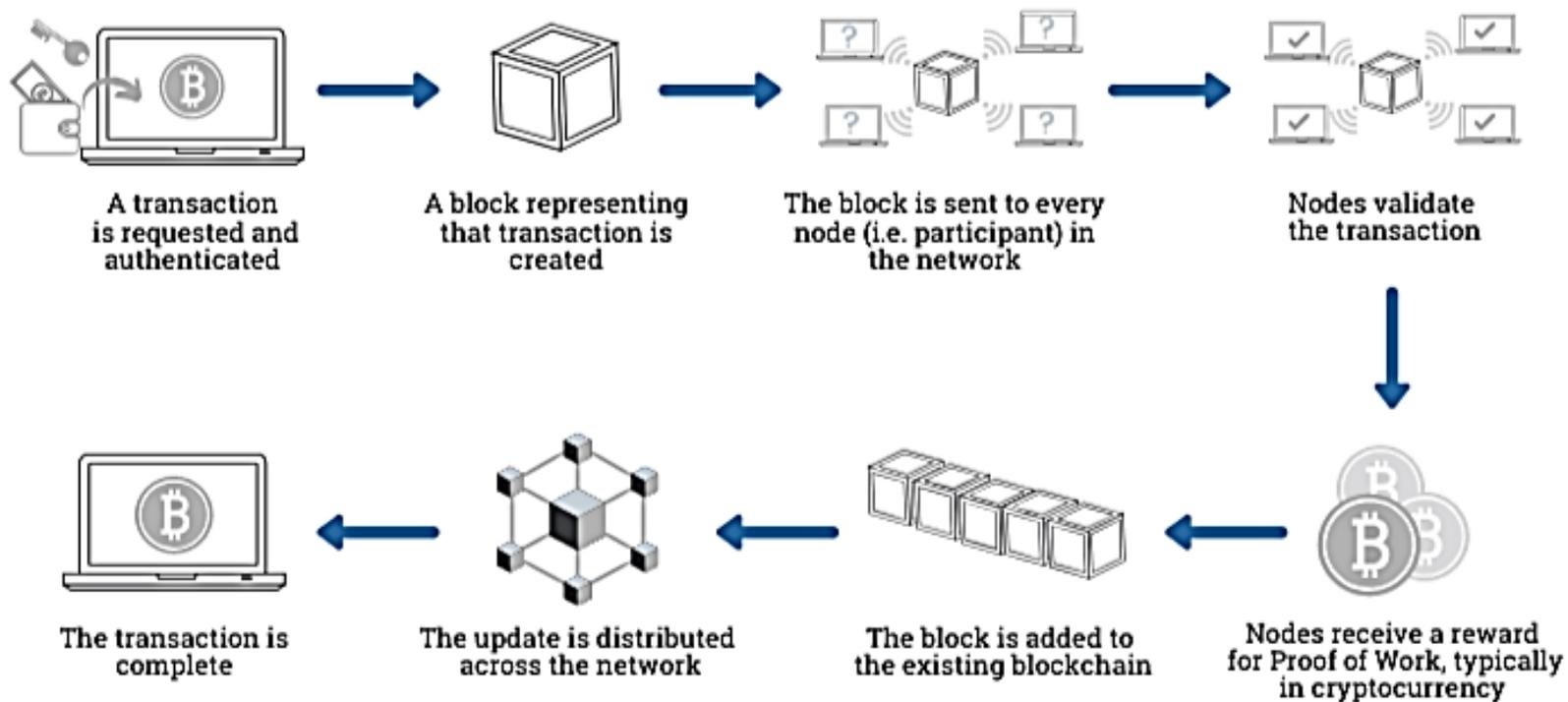
Los nodos validadores o mineros reciben una recompensa económica por ser los primeros en hacer estas 2 cosas:

1. Codificar las transacciones en un algoritmo SHA 256
2. Resolver el problema matemático de alta complejidad

También se gana el derecho de conectar ese bloque a la blockchain y enviar una copia actualizada a la red.



How does a transaction get into the blockchain?



© Euromoney Learning 2020

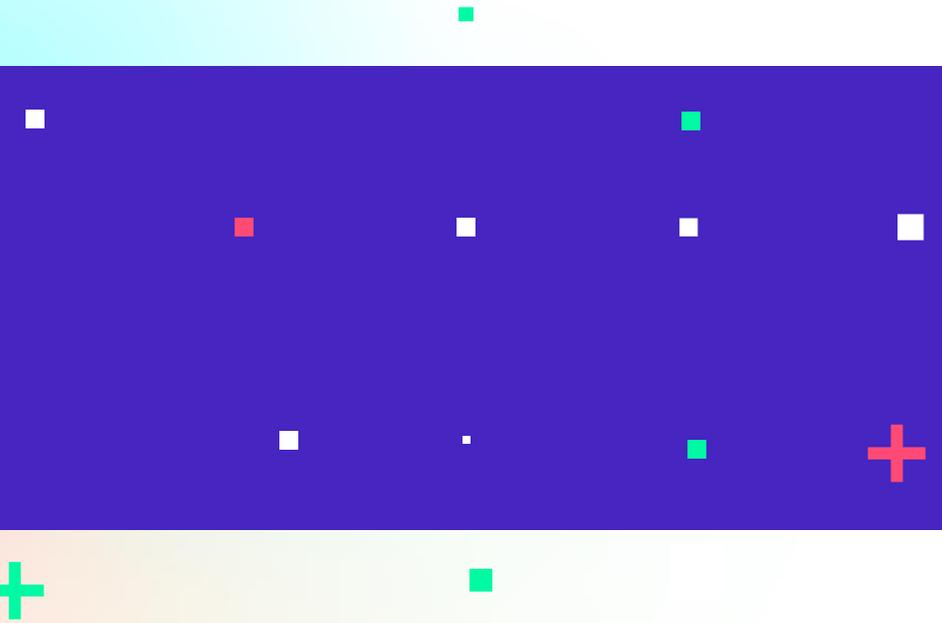
Ventajas

- Seguridad en la red
- Aumenta confianza entre pares
- Disminuye necesidad de órganos centrales
- Eficiencia en transferencia de recursos

Desventajas

- Coste energético aumenta con el tiempo
- Concentración progresivo de poder de minado.
- Velocidad de Transacciones por segundo procesadas es lento

Proof of stake



Los derechos de participar/votar como nodo se dá a traves del bloqueo parcial (Stake) de su recurso, demostrando el interés en sostener el proyecto.

De esta manera, más recurso en stake, más probabilidad en adicionar el siguiente bloque a blockchain.



Fuente: ledger.com

- Se utiliza un modelo determinístico para seleccionar a los nodos que verifican el bloque.
- No es necesaria una capacidad muy grande de computación
- Costos de mantener los nodos son relativamente muy bajos

Tipos de Blockchain

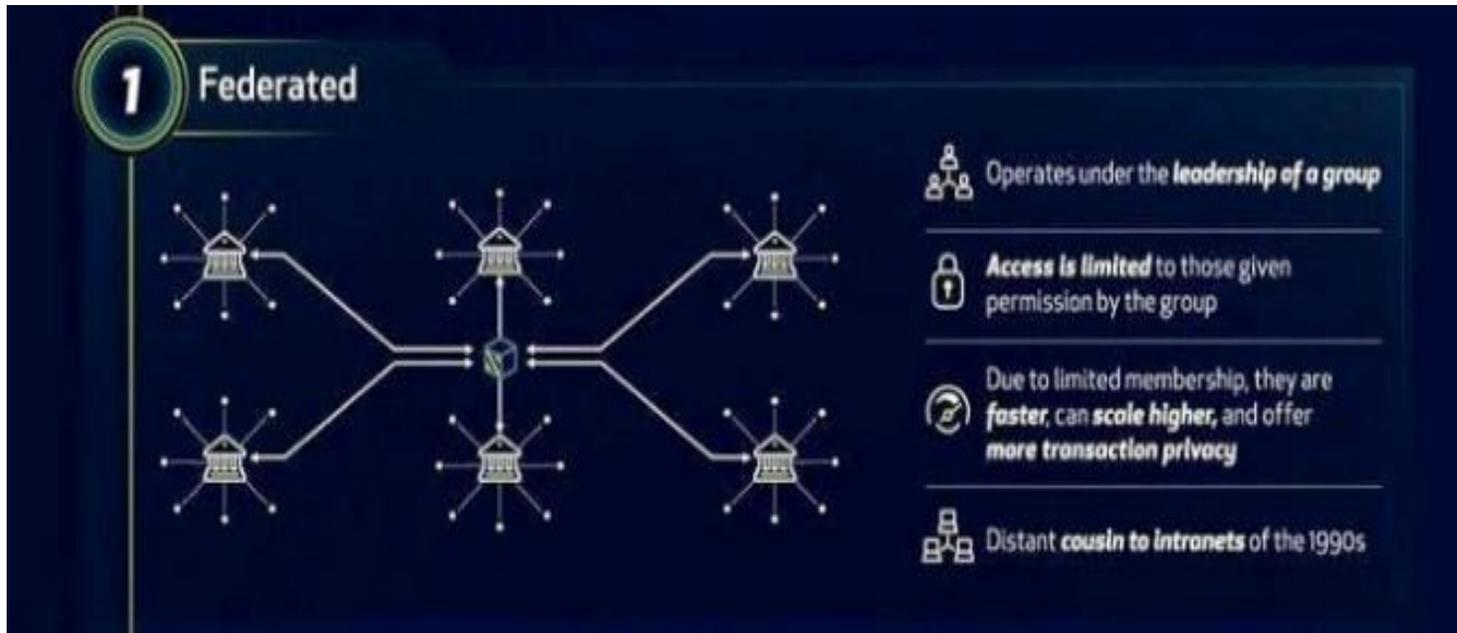


Tipos de Blockchain

1. Federadas o de consorcio
2. Privadas
3. Públicas



Blockchain Federada o de consorcio



- Lideradas por grupos empresariales
- Acceso limitado por el grupo
- Más rápidas, más escalables
- Transacciones verificadas por privados.

Usos: Banca, Seguros, Energético.

Fuente: Brave new coin, Entrepreneur

Blockchain Privadas

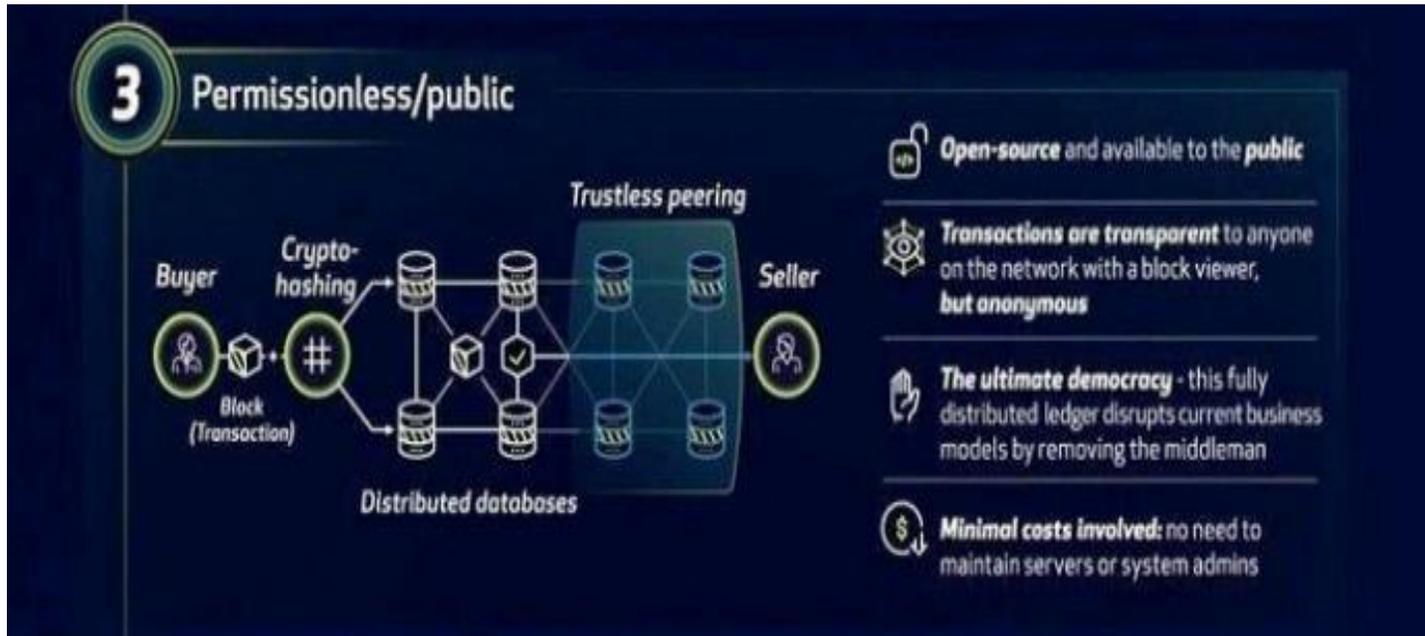


Fuente: Brave new coin, Entrepreneur

- Acceso puede ser Publico o Privado
- Ideal para temas de Identidad Digital
- Gestión de Privacidad en sector médico

Usos: Servicios legales, Servicios de compliance.

Blockchain Pública

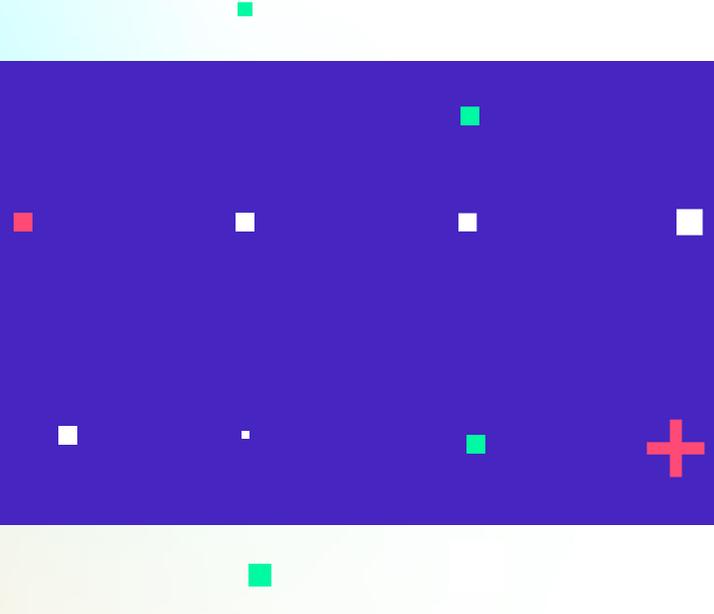


Fuente: Brave new coin, Entrepreneur

- Cualquiera puede participar en la red
- Mecanismo tipico de incentivación
- Cualquiera puede verificar las transacciones, estas son Pseudo Anónimas

Usos: Crypto monedas, Web 3, NFT

Casos de uso Colombia



1. Agencia Nacional de Tierras: Blockchain Pública para verificar autenticidad de los registros.
2. Supernotariado y Registro: Blockchain privada, para gestión y consulta de documentación.
3. Clinica las Americas Medellin: Blockchain privada para trazabilidad de insumos médicos.

Blockchain es una herramienta que crea un impacto positivo en múltiples sectores, generando confianza y mejorando procesos que tienen como resultado un aumento del bienestar poblacional. Es un mundo de oportunidades que promueve una descentralización sana y el desarrollo de una nueva economía.

¡Muchas Gracias!



@Morrislopez89



@Oscardefrancia



@Hashhouse.club

Expe riencia tech.2022

19 y 20 de oct.

Centro Empresarial El Poblado

Vive la evolución digital

