



Fundamentos de Blockchain en Algorand

Dra. Rocío A. Aldeco P.

Semestre 2023-1



Algorand
Centre of Excellence

¿Qué es Algorand?

- Algorand es una blockchain que aspira a ser la solución del trilema de blockchain con el uso del protocolo PoS y VRF (Función Aleatoria Verificable o *Verifiable Random Functions*).
- Soporta contratos inteligentes sobre su máquina virtual (AVM, Algorand Virtual Machine) y su moneda nativa es el ALGO.
- Algorand fue fundada en 2017 por Silvio Micali, un profesor del MIT.
- La red de prueba de Algorand fue lanzada al público en abril de 2019 y la red principal en junio de 2019.



Principales Características



Protocolo de Consenso

Usa el protocolo **Pure Proof of Stake**

La probabilidad de ser elegido es proporcional a la participación.

- Cada ALGO es un “billete de lotería”
- Usa la técnica denominada Función Aleatoria Verificable.

Consta de tres pasos

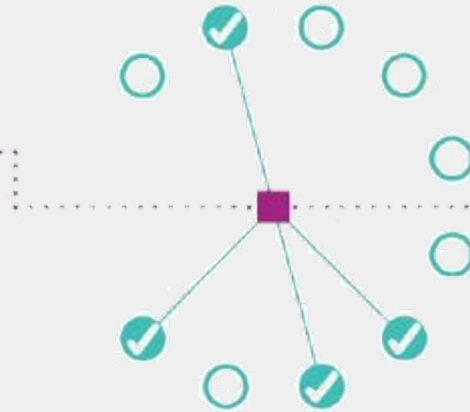
- Propuesta de Bloque
- Filtrado de Bloque
- Quórum y certificación



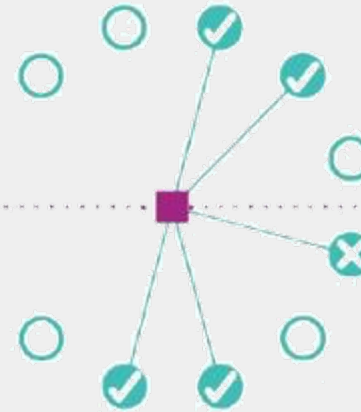
¿Cómo funciona PPOS?



Se elige una cuenta para proponer el bloque.



Se elige un comité para filtrar y votar las propuestas del bloque.



Un nuevo comité es elegido para votar sobre la aprobación del bloque



Bloque escrito en la cadena de bloques.

- Cada bloque tiene un nuevo proponente y nuevo comité, elegidos al azar utilizando VRF.
- Esto permite reemplazar a los verificadores, creando seguridad.
- Cualquiera que tenga un token puede participar.
- No es necesario calcular funciones difíciles ni consumir grandes cantidades de electricidad.
- El proceso completo dura aproximadamente 5 segundos.

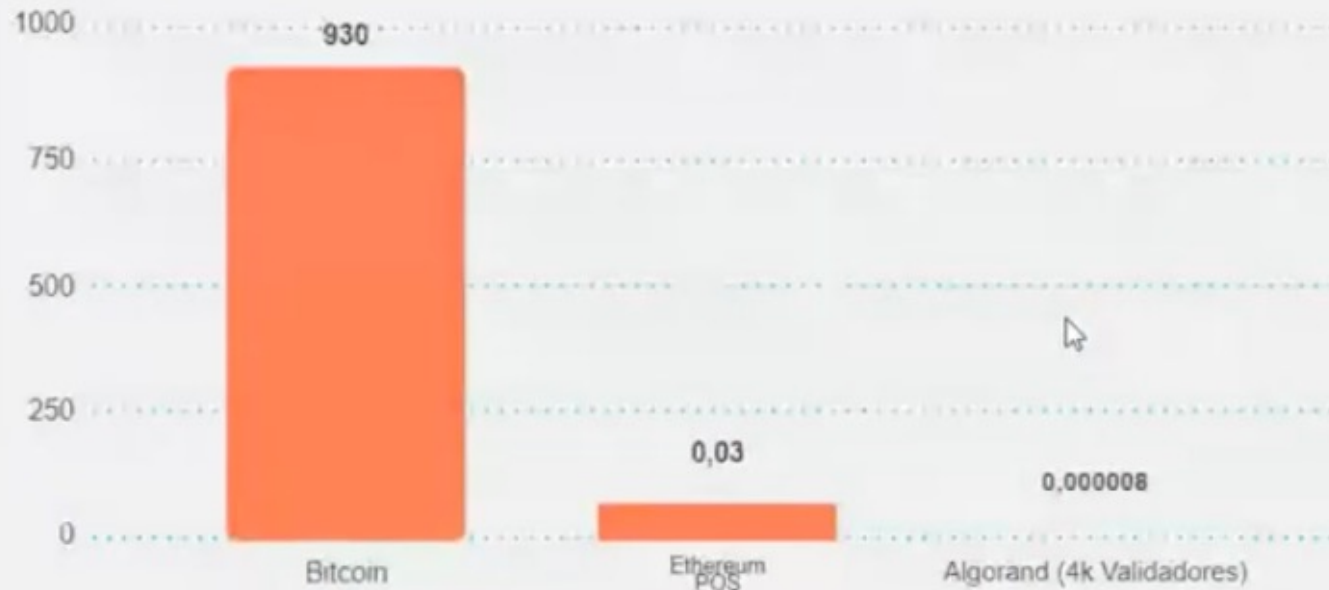


Huella de Carbono

Consumo promedio de energía por transacción (abril de 2021)

*Las transacciones de Algorand son todas definitivas

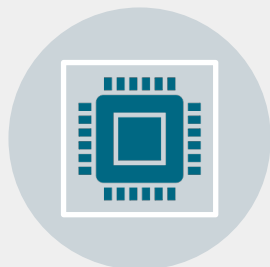
[kWh/txn]



<https://www.algorand.com/resources/blog/sustainable-blockchain-calculating-the-carbon-footprint>



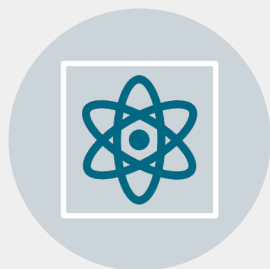
Funcionalidad



Contratos Inteligentes. Pueden desarrollarse en diversos lenguajes de programación para ejecutarse sobre la maquina virtual de Algorand (AVM).



Algorand Standard Assets (ASA). Un activo personalizado y fácil de crear.



Transferencias Atómicas. La posibilidad de integrar varias transacciones en un solo proceso atómico.



Cambio de llave (Rekeying). Cambiar la llave privada asociada a una llave pública las veces que sea necesario.

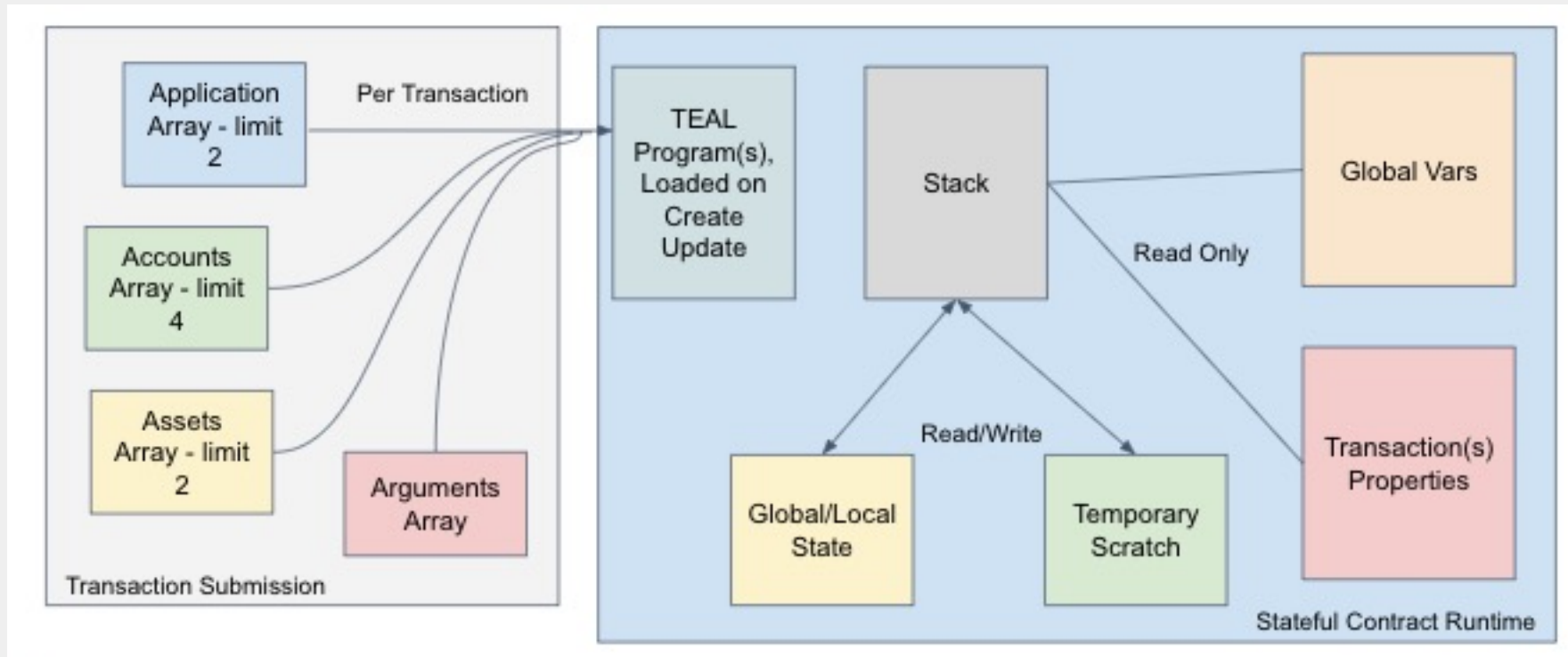


Contratos Inteligentes

SKDs Oficiales: JS, GO, Python y Java



SDKs de la comunidad: Dart, PHP, Rust, Unity, y .NET



Algorand Virtual Machine (AVM)



Algorand Standard Assets (ASAs)

FUNGIBLE TOKENS (FT)

- Criptomonedas
- Monedas Estables
- Puntos en un juego
- Puntos de fidelidad
- Créditos

NON FUNGIBLE TOKENS (NFT)

- Identidad
- Certificaciones
- Coleccionables
- Bienes raíces
- Artículos en un juego

RESTRICTED FUNGIBLE TOKENS (RFT)

- Dinero Fiduciario emitido por el gobierno
- Valor (acciones, títulos de créditos u obligaciones)

RESTRICTED NON FUNGIBLE TOKENS (RNT)

- Bienes Raíces
- Registros de propiedad
- Certificaciones reglamentarias

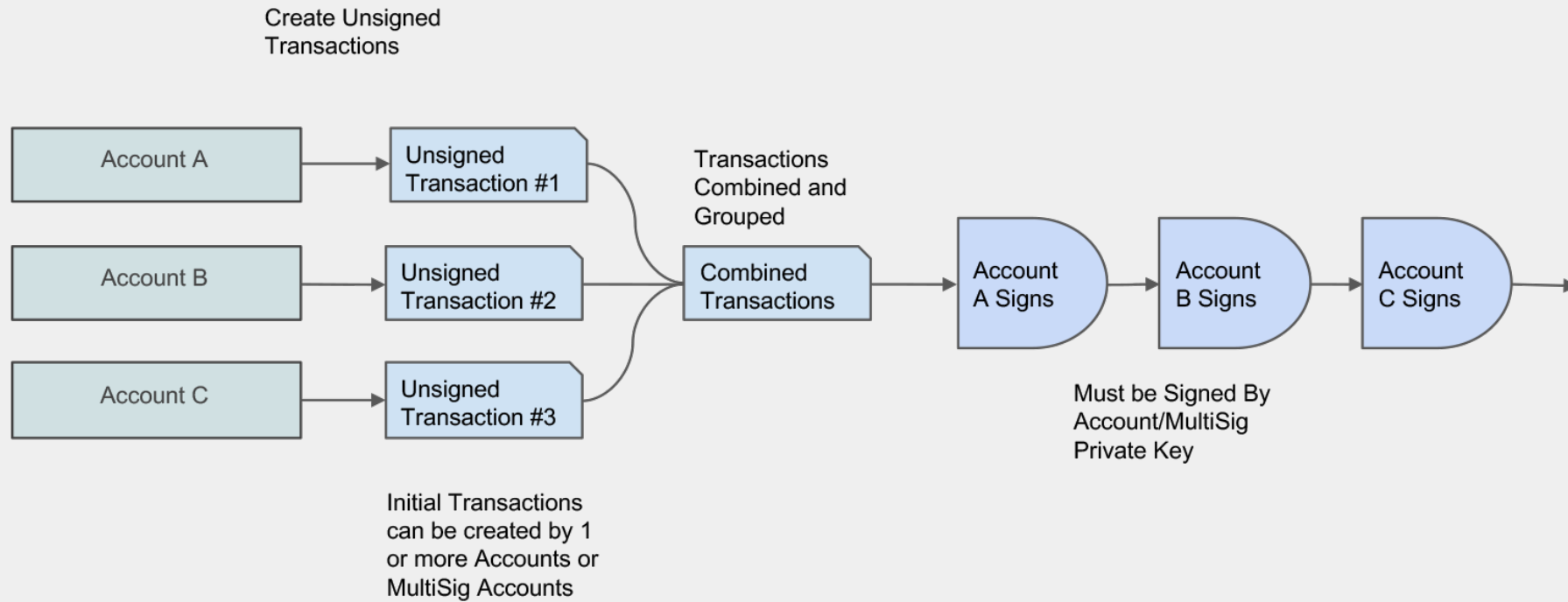


Transferencia Atómicas

- En las finanzas tradicionales, el comercio de activos suele requerir un tercero de confianza para asegurarse de que ambas partes reciben lo acordado.
- En Algorand esto se implementa como una **transferencia atómica**.
 - Un conjunto de transacciones se ven como una sola de tal manera que todas tienen éxito o todas fracasan.
 - Las transferencias atómicas permiten a completos desconocidos intercambiar activos sin necesidad de un intermediario de confianza.
- Las transferencias atómicas se pueden usar en casos como los siguientes.
 - **Operaciones circulares**: Alice paga a Bob si y sólo si Bob paga a Claire si y sólo si Claire paga a Alice.
 - **Pagos en grupo**: Todos pagan o nadie paga.
 - **Intercambios descentralizados**: Intercambiar un activo por otro sin pasar por un intercambio centralizado.
 - **Pagos distribuidos**: Pagos a múltiples destinatarios.
 - **Comisiones de transacción agrupadas**: Una transacción paga las comisiones de otras.

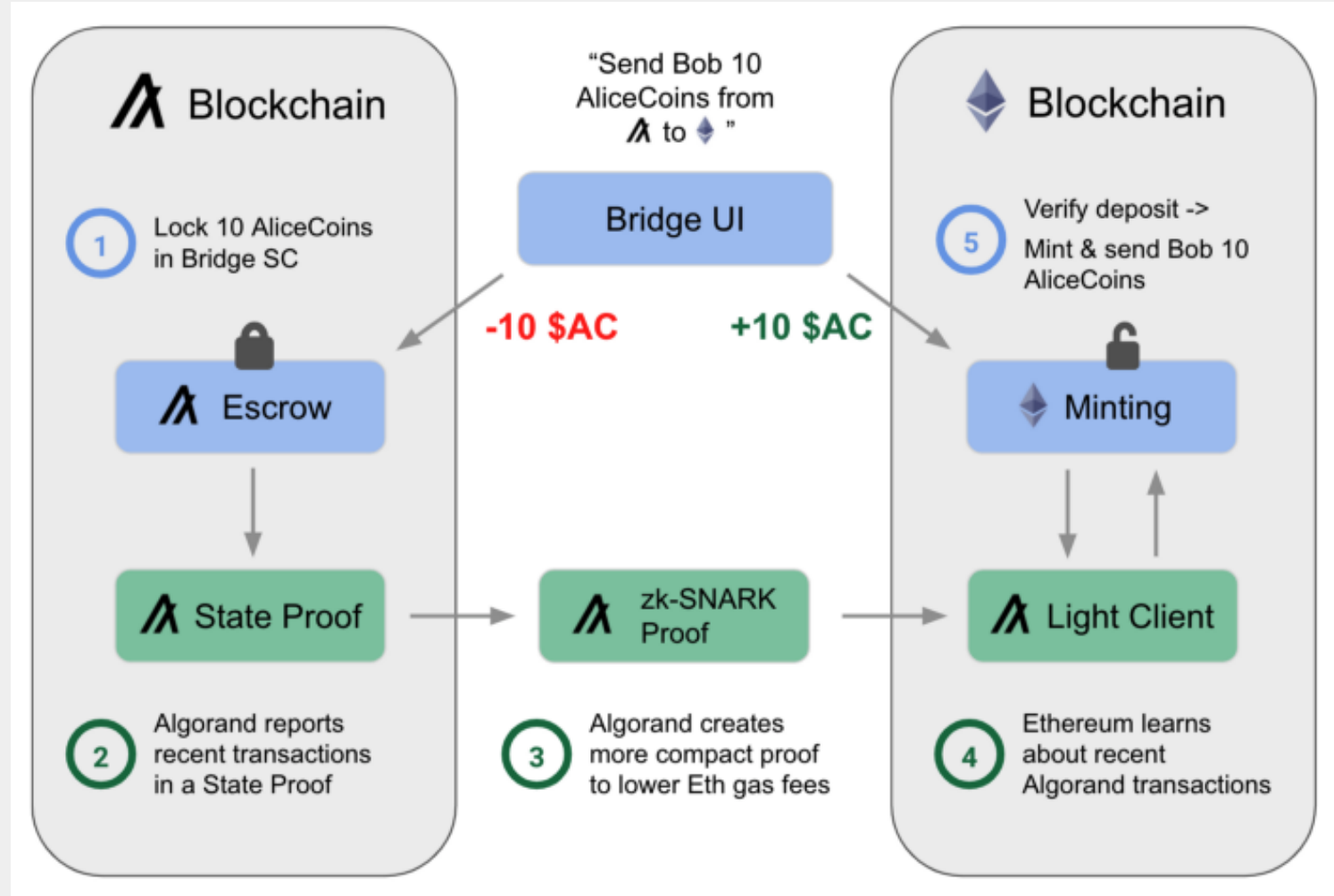


Transferencia Atómicas



Algoran State Proof (ASP)

- Conecta Algorand con el resto de las redes Blockchain.
- Los ASP son una cadena inmutable de pruebas que atestiguan el estado de la cadena de bloques de Algorand.
- Permiten a cualquiera realizar un seguimiento de las transacciones, saldos y datos de aplicaciones de Algorand en entornos de bajo consumo, como un teléfono, un smartwatch e incluso dentro de un contrato inteligente de blockchain, sin comprometer la seguridad.



Ecosistema



Lofty Marketplace About us Learn Blog Sell my property Log In Sign Up

1248 S Keeler Ave
Chicago, IL 60607

18.90% IRR
7.90% CoC

88%
885 tokens left

5401 Odom Ave
West Adams, IL 60638

19.10% IRR
7.43% CoC

80%
4579 tokens left

3427 Sturdevant St
Ballerup, IL 60604

17.91% IRR
7.58% CoC

100%
0 tokens left

<https://www.lofty.ai/>

travelX Menu

Reimagining travel, together!

travelX is building the new blockchain-based distribution and retailing infrastructure for the travel industry.

<https://www.travelx.io/>

New Learn how to be part of the real economy here. >>

The first global tokenization infrastructure for agrocommodities.

We create a secure and frictionless ecosystem to make trading grains easier, more efficient and more reliable.

Contact us

What is Agrotoken?

Agrotoken Quote

SOYA: USD 382,88

CORA: USD 240,32

WHEA: USD 350,33



WAYRU Pre-sale HOTSPOTS POOLS TOKEN AIRLOCKS TEAM EN

DECENTRALIZED INTERNET NETWORK
POWERED BY YOU
DISRUPTING THE STATUS QUO OF INTERNET ACCESS

Buy and Earn Lite Paper

<https://www.wayru.io/>

Derechos de autor / Propiedad intelectual

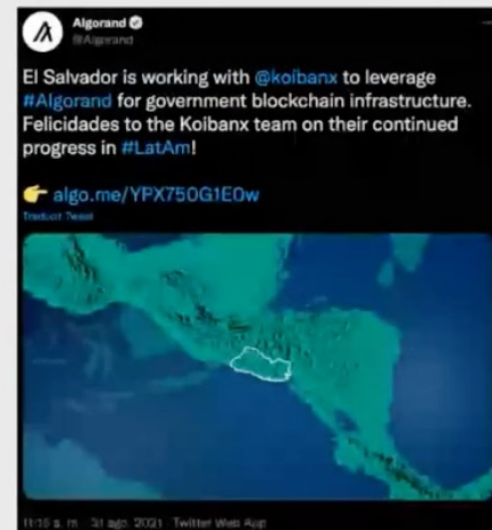
SIAE DALLA
PARTE
DI CHI
CREA

Propiedad Intelectual en Nigeria NG



<https://twitter.com/Algorand/status/1529113744672006144>

Infraestructura Blockchain en El Salvador sv



Clima



DeFi



AlgoFi Money Market



Folks Finance Money Market



AlgoGARD Money Market



Pact DeX (AMM)



HumbleSwap DeX (AMM)



Tinyman DeX (AMM)



WAGMI Swap DeX (AMM)



AlgoDEX DeX (Order Book)



AlgoMint Bridge



Yieldly Staking

Stablecoins



Tether USD

Tether es un emisor de stablecoins líder en el mercado que lanzó la mayor stablecoin por capitalización de mercado, Tether USD, en 2014.



USD Coin

USDC es una stablecoin respaldada por el dólar estadounidense, lanzada por los pioneros del sector Coinbase y Circle.



QCAD

QCAD es la primera stablecoin no respaldada por el dólar estadounidense que se emite en Algorand. lo que permite un par sintético de negociación USD/CAD en la red.



BRZ

La primera stablecoin respaldada por el real brasileño en Algorand.

Creadores



dartroom



AlgoGems



Abris



Rand Gallery



Republic



aorist



zestbloom



AB2 Gallery

Musica

Opulous
Musica MFTsDequency
Sincronización musical
mercado de licencias

STOI

STOI
Contrato inteligente basado e
la propiedad de la canción

Musica



Inmobiliaria

Lofty
Finca raíz residencialPocket Properties
Finca raíz residencialSliceSpace
Finca Raíz Comercial

Algunas métricas

Transactions (7D)

7,964,815



Total Addresses

27,363,569



Nodes (7D)

1,807



Total Value Locked

\$311,952,422



Total ASAs

5,802,506



BLOCK SPEED

3.7 sec

TPS

11.58

TX COST

\$0.00032

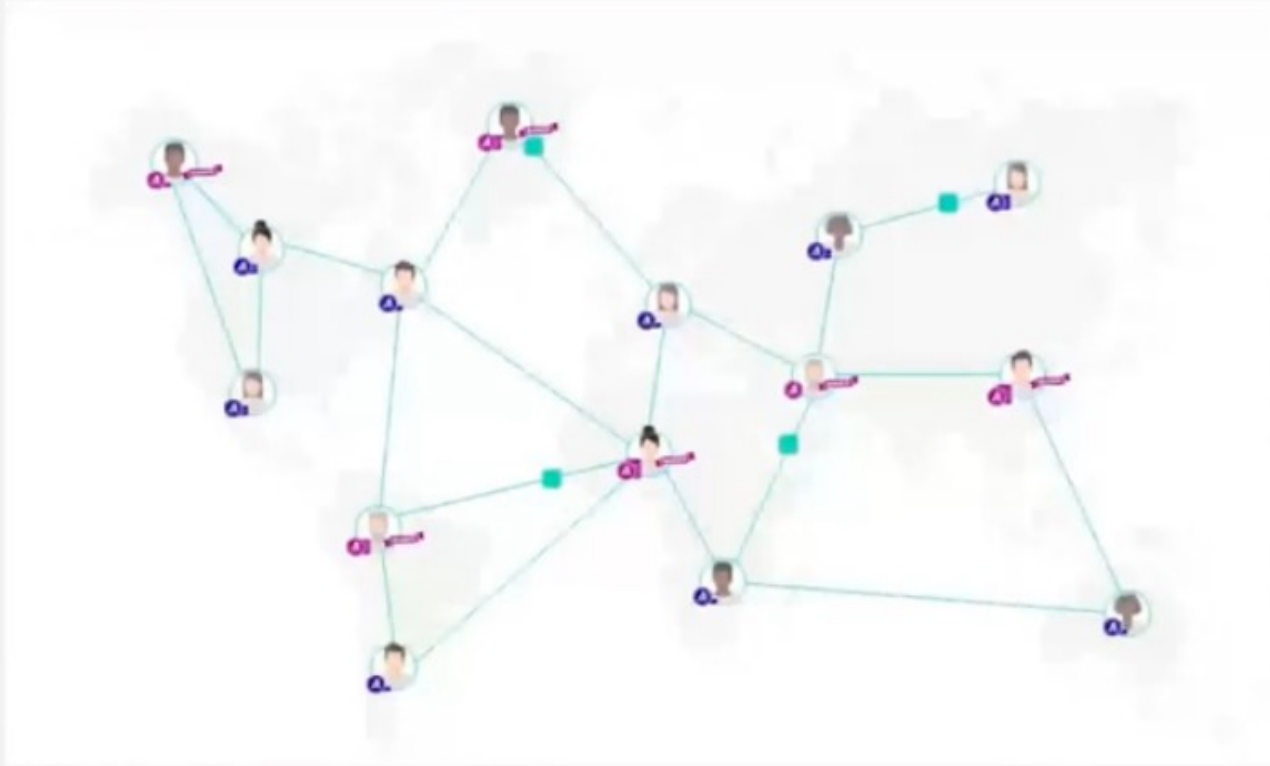
ACCOUNTS

27,275,418

<https://metrics.algorand.org/#/>

<https://algoexplorer.io/>

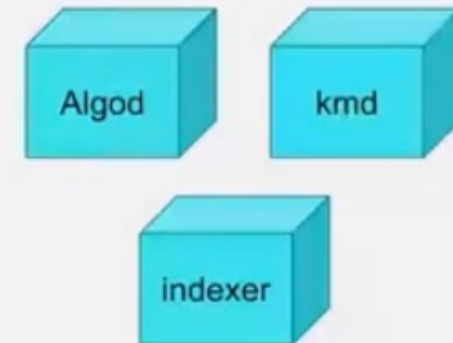
Donde se ejecuta Algorand



Requisitos:

- 4GB RAM
- 100Mbps connection
- 200MB HDD

Daemons:



Cómo interactuar con la red de Algorand



Tu propio
nodo



Nodo y
servicio de
tercero



Sandbox: Red y
nodo local
privado



Requerimientos

- En Mac se recomienda instalar Brew.
- Python 3.8 o superior
- Node JS
- SDK Python



Recursos

- Discord
 - discord.gg/Algorand
- Página para desarrolladores
 - developer.algorand.org
- YouTube
 - [YouTube/Algorand](https://www.youtube.com/Algorand)
- Twitter
 - [@AlgoDevs](https://twitter.com/AlgoDevs)



Redes Sociales

