

ALGORAND



Weimar Quintero Calle
Universidad de Antioquia
weimar.quintero@udea.edu.co



Algorand

Algorand es una red blockchain y un proyecto fundado en 2017 por el profesor **Silvio Micali**, un científico informático del MIT. La red principal se lanzó en junio de 2019 junto con su criptomoneda nativa, **ALGO**.

Plataforma de contratos inteligentes que utiliza un protocolo de blockchain de código abierto, sin permisos y basado en **Pure-Proof-of-Stake (PPoS)**.





Ventajas



Seguridad Mejorada: Gracias a su protocolo Pure Proof-of-Stake (PPoS), Algorand ofrece una alta seguridad al seleccionar nodos de validación de manera aleatoria, lo que dificulta los ataques.



Descentralización: Cualquier nodo en su red puede participar en el proceso de consenso sin necesidad de equipos especiales o un alto consumo de energía.



Transacciones Rápidas y Económicas: Las transacciones en Algorand son rápidas, con tiempos de confirmación de alrededor de 5 segundos, y las tarifas son muy bajas.



Escalabilidad: Algorand está diseñado para manejar una gran cantidad de transacciones por segundo (TPS) sin sacrificar la descentralización.



Código Abierto: La blockchain de Algorand es pública y de código abierto, lo que promueve la transparencia y la colaboración en la comunidad.

Desventajas



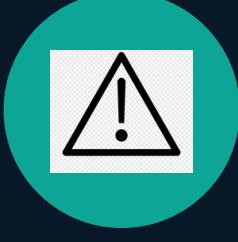
La red Algorand está administrada por 140 nodos de retransmisión autorizados y controlados por la Fundación Algorand, a los que también se les otorgaron rondas de inversión temprana preferencial y asignaciones futuras de tokens predeterminadas.



Algorand sufre una distribución de tokens extremadamente concentrada en la que más del 60% del suministro de tokens está controlado por fundadores y personas con información privilegiada privadas.

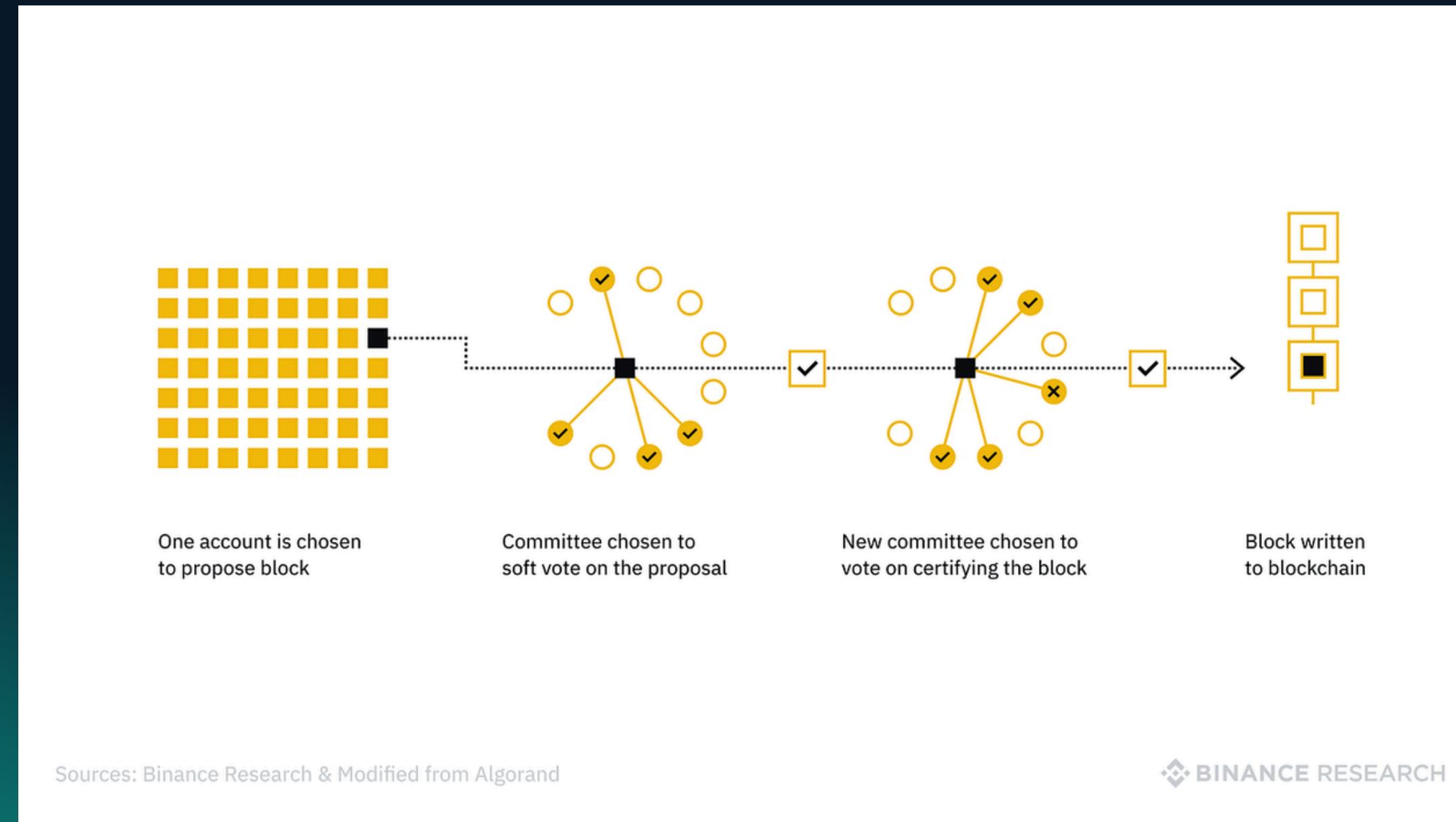


A pesar de haberse lanzado recién en 2019, la “hinchazón estatal” de Algorand ya es peor que la de Bitcoin (13 años de historia) y Ethereum (7 años de historia), lo que requiere hardware más especializado para mantener la historia de la cadena, lo que lleva a una mayor centralización.



Algorand se lanzó a un sector abarrotado y no logró obtener una adopción ni tracción significativas, al igual que otras cadenas de bloques de contratos inteligentes que se lanzaron en un momento similar (Solana, Terra, Avalanche) sí lo hicieron.

Mecanismo de consenso



Algorand creó una versión única de un algoritmo de gobernanza mediante la implementación de Pure-Proof-ofStake (PPoS). Los miembros de la red solo necesitan tener tokens ALGO para poder participar. PPoS opera en dos etapas:

Etapa 1: Se selecciona aleatoriamente un token ALGO de los tokens disponibles. El dueño de este token propone el próximo bloque.

Etapa 2: Se eligen al azar miles de tokens para votar, validar y aprobar el bloque. Cuantos más tokens tenga un participante, mayor será la probabilidad de ser seleccionado.

Tipos de nodos

Los nodos de **retransmisión** actúan como centros de red, comunicándose con grupos de nodos de participación para enrutar bloques.

Los nodos de **participación** se conectan a otros nodos similares, pero solo tienen un nodo de retransmisión conectado a la vez. Aunque tienen menos responsabilidades, estos nodos aún pueden participar en el consenso de la red.



ALGO

ES LA CRIPTOMONEDA NATIVA DE ALGORAND Y TIENE UN SUMINISTRO MÁXIMO TOTAL DE 10 MIL MILLONES DE MONEDAS, QUE SE DISTRIBUIRÁN HASTA 2030

Se utiliza principalmente en la red para ejecutar contratos inteligentes, pagar tarifas de gas y realizar transacciones. Esto impulsa una variedad de aplicaciones descentralizadas (dApps), mercados, intercambios y más. Las tarifas en la red no solo se procesan rápidamente (con tiempos de bloque inferiores a 5 segundos), sino que también son muy asequibles, costando solo 0,001 ALGO por transacción.



ALGO

Como muchas otras criptomonedas nativas, ALGO tiene tres usos principales:

1. ALGO se utiliza para pagar las tarifas de transacción en la red Algorand. Comparado con redes como Ethereum (ETH) y Bitcoin (BTC), Algorand ofrece tarifas muy bajas. Desde enero de 2022, cada transacción cuesta solo 0.0014.
2. ALGO puede ser apostado para tener la oportunidad de ser seleccionado como proponente o validador de bloques.
3. ALGO se puede mantener en una billetera sin custodia para ganar recompensas con cada bloque que se añade exitosamente a la cadena.



Debilidades

Un grupo cerrado de nodos/validadores

Los primeros usuarios de Algorand no solo se llevaron una buena parte de las recompensas, sino que también obtuvieron el derecho a manejar los nodos de retransmisión de Algorand.

Inicialmente, se eligieron 100 entidades para manejar estos nodos de retransmisión. Esto les da la oportunidad de obtener una gran parte del mercado si deciden no vender nunca. En 2021, se lanzó un programa piloto que permitió a nuevas entidades ofrecerse como voluntarias para manejar un nodo de retransmisión. Gracias a este programa, ahora hay 40 nuevas entidades (también seleccionadas a mano) que están manejando nodos de retransmisión, elevando el total a 140.



Debilidades

Pobre resistencia a la censura

Desde el punto de vista de un criptoentusiasta idealista, Algorand tiene varias fallas, como:

- Los nodos de retransmisión están autorizados y controlados por la Fundación.
- Se destinan 200 millones de ALGO a incentivos para patrocinadores tempranos/nodos de retransmisión (solo las entidades cercanas a la Fundación y aprobadas por ella pueden ejecutar un nodo de retransmisión para obtener estas recompensas).
- Hay una empresa con fines de lucro (Algorand, Inc.) detrás del proyecto, con sus propios directivos.
- Más del 50% del suministro de tokens está controlado por fundadores y personas con información privilegiada.
- La fundación puede congelar cuentas y hacer recuperaciones.
- Existe un documento formal (creado y votado por los primeros inversores) que describe cómo los primeros inversores pueden/venderán ALGO con ganancias (EIP-11252019AF: Adquisición acelerada condicional de derechos).



Debilidades

Escalamiento a corto plazo para problemas a largo plazo

Una debilidad más para Algorand es el problema de la “inflación de estados” y la sostenibilidad de la red. El crecimiento de estados se refiere a qué tan rápido aumenta la carga computacional de la blockchain. Los nodos completos (nodos de retransmisión en Algorand) almacenan todo el historial de la red desde el principio y deben poder validar todo el estado de la red. Cuantos más estados haya en una red, más potencia computacional necesitará un nodo para participar o validarla.



Posibles Soluciones

Descentralización de nodos:

Ampliar la cantidad de nodos de retransmisión permitiendo que más participantes se unan sin necesidad de aprobación centralizada. Esto podría lograrse mediante un proceso de selección más abierto y transparente. Para ampliar la cantidad de nodos de retransmisión, Algorand podría implementar un proceso de selección más abierto y transparente. Esto podría incluir la eliminación de barreras de entrada para nuevos nodos y la creación de un sistema de votación comunitaria para la aprobación de nuevos nodos. Además, podrían establecerse requisitos técnicos mínimos que sean accesibles para una mayor cantidad de participantes, promoviendo así una red más descentralizada.



Posibles Soluciones

Incentivos para nuevos nodos:

Ofrecer incentivos adicionales para que nuevos nodos se unan a la red, reduciendo la dependencia de los nodos iniciales y fomentando una mayor participación. Algorand podría ofrecer incentivos adicionales, como recompensas en ALGO, para motivar a nuevos participantes a unirse a la red como nodos de retransmisión. Estos incentivos podrían estar diseñados para ser atractivos tanto para pequeños operadores como para grandes entidades, asegurando una mayor diversidad y descentralización en la red.



Posibles Soluciones

Transparencia y gobernanza comunitaria:

Implementar un sistema de gobernanza más inclusivo donde la comunidad tenga mayor voz y voto en las decisiones importantes, reduciendo el control centralizado. Algorand podría desarrollar un sistema de gobernanza más inclusivo, donde la comunidad tenga una mayor voz en las decisiones importantes. Esto podría incluir la creación de un consejo de gobernanza elegido por la comunidad, la implementación de votaciones descentralizadas para decisiones clave y la publicación transparente de todas las decisiones y procesos de gobernanza. De esta manera, se reduciría el control centralizado y se aumentaría la confianza en la red.



Posibles Soluciones

Optimización del almacenamiento:

Implementar técnicas de compresión y poda de datos para reducir la carga de almacenamiento en los nodos. Esto puede incluir la adopción de soluciones como los rollups o las cadenas laterales (**sidechains**). Para reducir la carga de almacenamiento en los nodos, Algorand podría implementar técnicas de compresión de datos y poda de estados antiguos que ya no son necesarios para la validación actual. Soluciones como los rollups, que agrupan múltiples transacciones en una sola, o las cadenas laterales (**sidechains**), que permiten manejar transacciones fuera de la cadena principal, podrían ser adoptadas para mejorar la eficiencia del almacenamiento.



Posibles Soluciones

Mejora de la eficiencia:

Desarrollar y adoptar mejoras en el protocolo que aumenten la eficiencia de la red sin sacrificar la descentralización. Esto puede incluir la optimización del consenso y la reducción de los requisitos de hardware para los nodos. Algorand podría trabajar en la optimización de su protocolo de consenso para aumentar la eficiencia sin sacrificar la descentralización. Esto podría incluir la investigación y desarrollo de nuevos algoritmos de consenso que sean más rápidos y menos exigentes en términos de recursos. Además, la reducción de los requisitos de hardware para los nodos podría hacer que más personas puedan participar en la red, aumentando así la descentralización y la resiliencia de la red.





ALGORAND

GRACIAS...