# ALGORAND

**Weimar Quintero**
Universidad de Antioquia, Colombia
weimar.quintero@udea.edu.co

## Abstract

En el ámbito de blockchain, un **ledger** es un registro digital que guarda todas las transacciones realizadas en una red de blockchain. Este libro mayor es compartido y mantenido por todos los miembros de la red, asegurando que todos tengan una copia idéntica y actualizada de las transacciones.

**Algorand** es una forma democrática y eficiente de implementar un ledger. A diferencia de las implementaciones basadas en prueba de trabajo, Algorand requiere muy poca computación y genera un historial de transacciones que casi nunca se bifurca. Utiliza aleatoriedad algorítmica para seleccionar verificadores que construyen el siguiente bloque de transacciones válidas, garantizando que estas selecciones sean inmunes a manipulaciones y transparentes para todos los usuarios. En este documento, exploraremos sus principales características, así como sus debilidades y las posibles soluciones para abordarlas.

## 1 Introducción

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**. Tambien podemos definir Algorand como una plataforma de contratos inteligentes de nivel 1 que utiliza un protocolo de blockchain de código abierto, sin permisos y basado en Pure-Proof-of-Stake (PPoS). La red de Algorand opera con su propia criptomoneda nativa, ALGO. Mediante la asignación de ALGO, los usuarios pueden realizar transacciones peer-to-peer (P2P), impulsar aplicaciones descentralizadas (dApps) en la cadena, o simplemente apostar ALGO en la red principal para contribuir a la seguridad de la red y recibir recompensas inflacionarias a cambio. Fue diseñada para asegurar una verdadera descentralización, escalabilidad y seguridad para aplicaciones industriales.

Su principal objetivo es ofrecer una plataforma de contratos inteligentes robusta, de código abierto y accesible en el ámbito de las criptomonedas. Su moneda nativa, ALGO, respalda el creciente ecosistema de protocolos, mercados y aplicaciones descentralizadas (dApps). Algorand actúa como una plataforma de dinero digital, con ALGO impulsando su economía.

Aunque es un proyecto joven, Algorand ya se ha implementado en varios casos de uso reales, como el soporte de la billetera Bitcoin en El Salvador y una plataforma descentralizada para transacciones de atención médica. A medida que su ecosistema sigue creciendo, la blockchain de Algorand ya está cumpliendo con su propósito original y ademas resuelve el **trilema** de la arquitectura blockchain.

## 2 Ventajas y Desventajas

### 2.1 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 ataques1.
- Descentralización: Cualquier nodo en su red puede participar en el proceso de consenso sin necesidad de equipos especiales o un alto consumo de energía1.
- Transacciones Rápidas y Económicas: Las transacciones en Algorand son rápidas, con tiempos de confirmación de alrededor de 5 segundos, y las tarifas son muy bajas1.
- 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.

### 2.2 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(per cent) 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.

## 3 Mecanismo de consenso

Algorand creó una versión única de un algoritmo de gobernanza mediante la implementación de Pure-Proof-of-Stake (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.

Este proceso permite que todos los titulares de ALGO participen directamente en la gobernanza, proporcionando descentralización mediante la selección aleatoria de tokens en lugar de delegados. También proporciona seguridad, ya que reconoce la posible presencia de malos actores, pero limita su influencia a través de un proceso aleatorio y seudónimo. Con solo tokens seleccionados, es imposible realizar DDoS en los nodos más ocupados de la red. Finalmente, Algorand logra escalabilidad gracias a la selección de lotería casi instantánea que se ejecuta de manera independiente entre nodos, lo que aumenta significativamente la velocidad de propagación de bloques.

### 3.1 ¿Cómo funciona?

A diferencia de las cadenas de bloques de Prueba de Participación (PoS), Algorand no exige una participación mínima, eliminando una barrera de entrada significativa para el usuario promedio. En PoS, la escalabilidad a menudo se logra a costa de que unos pocos validadores con grandes participaciones dominen las aprobaciones de bloques. La Prueba de Trabajo (PoW) enfrenta un problema similar, ya que los grandes grupos de minería casi siempre ganan la carrera para crear nuevos bloques.

La clave de la escalabilidad de Algorand radica en su mecanismo de consenso de Prueba de Participación Pura (PPoS). Este protocolo permite procesar muchas transacciones rápidamente sin sacrificar la descentralización. En Algorand, los validadores y proponentes de bloques se eligen aleatoriamente entre todos los que han apostado y generado una clave de participación. La probabilidad de ser elegido está directamente relacionada con la proporción de la participación del participante en el monto total apostado.

*Aunque un pequeño poseedor tiene menos posibilidades de ser seleccionado que un gran poseedor, cada staker que ejecuta un nodo es un posible validador. Esto hace que la seguridad de la red esté más descentralizada en comparación con un conjunto elegido de validadores, como en la prueba de participación delegada.*

Cuando los usuarios apuestan y generan su clave de participación, se convierten en nodos de participación. Estos nodos se comunican a través de los nodos de retransmisión de Algorand. Durante la fase de propuesta de bloque, se seleccionan varios proponentes de bloque mediante una función aleatoria verificable (VRF), que toma en cuenta la proporción de la participación de cada validador. La identidad de los proponentes de bloque se mantiene en secreto hasta que se propone el nuevo bloque, lo que mejora la seguridad de la red al evitar ataques maliciosos contra el validador elegido. No obstante, un proponente puede demostrar su legitimidad mostrando su salida VRF junto con el bloque propuesto. Después de que se envía un bloque, se eligen aleatoriamente nodos de participación para formar parte del comité de votación suave. Esta fase filtra las propuestas, permitiendo que solo un candidato las agregue a la cadena de bloques. El poder de voto en este comité es proporcional a la cantidad apostada por cada nodo, y los votos se utilizan para seleccionar el bloque propuesto con el hash VRF más bajo. Esto garantiza que no se pueda atacar preventivamente al proponente de un bloque, ya que el hash VRF más bajo es un valor impredecible. Después de la etapa anterior, se forma un nuevo comité para verificar la integridad de las transacciones y evitar el doble gasto en el bloque. Si el comité valida el bloque, este se agrega a la cadena. Si no, el bloque es rechazado, la cadena de bloques entra en modo de recuperación y se selecciona un nuevo bloque. No hay penalización para el líder que propone un bloque defectuoso, lo que es un aspecto controvertido del mecanismo de consenso PPoS. La posibilidad de una bifurcación en

Algorand es extremadamente baja, ya que solo una propuesta de bloque llega a la etapa de certificación a la vez. Una vez agregado el bloque, todas las transacciones se consideran finales.

# 4 Tipos de nodos

La red Algorand se compone de dos tipos de nodos: nodos de **retransmisión** y nodos de **participación**. 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.

Según la documentación de Algorand, un nodo es considerado un nodo de retransmisión válido si cumple con dos condiciones:

**1.** Está configurado para aceptar conexiones entrantes en un puerto de acceso público (por convención, el puerto 4161).

**2.** Su dirección IP pública (o un nombre DNS válido) y el puerto asignado están registrados en los registros SRV de Algorand para una red específica (MainNet/TestNet).

Un nodo de retransmisión debe ser capaz de soportar muchas conexiones y manejar la carga de procesamiento de los datos que fluyen hacia y desde estas conexiones. Por lo tanto, requieren significativamente más energía que los nodos de participación. Los nodos de retransmisión siempre se configuran en modo de archivo.

# 5 ¿Qué es ALGO?

ALGO es la criptomoneda nativa de Algorand y tiene un suministro máximo total de 10 mil millones de monedas, que se distribuirán hasta 2030. Con cada nuevo bloque forjado, se envía nuevo ALGO a billeteras específicas que ya contienen ALGO. Para recibir estas recompensas, debes tener al menos 1 ALGO en una billetera sin custodia. Estas recompensas pueden generar un rendimiento anual (APY) de aproximadamente 5-8(per cent) para los titulares de ALGO y se distribuyen aproximadamente cada 10 minutos. Este mecanismo convierte a ALGO en una de las criptomonedas más sencillas para generar ingresos pasivos, ya que permite el "staking pasivo" del token. ALGO 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.

## 5.1 Principales casos de uso de 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.

*El tercer uso es un gran incentivo para que el usuario promedio invierta en ALGO. No es necesario interactuar con una aplicación descentralizada (DApp) para apostar las monedas ni esperar un período de bloqueo para empezar a ganar. Todo se gestiona automáticamente mediante contratos inteligentes. Además, Algorand publica una lista de proyectos que adoptan su tecnología blockchain, muchos de los cuales requieren el uso de ALGO.*

# 6 Casos de Uso Algorand

## 6.1 Caso de uso principal

El objetivo principal de Algorand es ser la plataforma de contratos inteligentes más fuerte, abierta y accesible en el mundo cripto. La moneda de la red, ALGO, se usa mucho para apoyar el ecosistema en crecimiento de protocolos, mercados y aplicaciones descentralizadas. Básicamente, Algorand es una plataforma de dinero digital y ALGO es la moneda que impulsa su economía. Aunque es un proyecto joven, Algorand ya se usa en varios casos reales. Desde soportar la billetera Bitcoin en El Salvador hasta ofrecer una plataforma descentralizada para transacciones de salud. Aunque el ecosistema sigue creciendo, la blockchain de Algorand ya se usa como se planeó.

## 6.2 Casos de uso secundarios

Además de ser la base del ecosistema Algorand como plataforma monetaria, ALGO también se puede usar para:

- Participar en la gobernanza de Algorand.
- Hacer transacciones entre pares (P2P).
- Soportar redes con permisos.

Cualquier billetera ALGO con al menos un ALGO, incluso en exchanges como Coinbase, puede recibir recompensas inflacionarias. Al hacer staking de ALGO en una billetera compatible, el nuevo modelo de gobernanza de Algorand permite que todos los titulares participen.

### 6.3 Desafíos para la adopción

Algorand ha creado una blockchain de capa 1 confiable que ha crecido mucho en el mercado cripto actual. Pero aún enfrenta varios desafíos importantes mientras sigue desarrollándose:

- El espacio de blockchain L1 está lleno y es muy competitivo.
- Algorand sigue siendo un proyecto joven y está detrás de otros L1 en dApps, DeFi, desarrolladores, usuarios y otras métricas clave.
- Algorand tiene una distribución de tokens pobre y está más centralizado que muchos competidores.
- Algorand no puede aprovechar los beneficios de la máquina virtual de Ethereum (EVM) como Binance Chain, Fantom, Avalanche y otros.

## 7 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. Este grupo inicial incluye a los primeros inversores, universidades y empresas privadas que se comprometieron a mantener la infraestructura de nodos de retransmisión de Algorand hasta 2024. Después de 2024, estos participantes pueden decidir si quieren seguir manejando los nodos de retransmisión o no.

La red Algorand tiene dos tipos de nodos: los nodos de participación, que son fáciles de configurar y tienen requisitos básicos, y los nodos de retransmisión, que necesitan la aprobación de la Fundación Algorand y requieren mucho más capital y potencia informática. Según la Fundación Algorand, los nodos de retransmisión deben tener al menos:

- 8 CPU virtuales
- 16 GB de RAM
- Disco duro de alto rendimiento de 1 TB
- Al menos 5 TB de tráfico de salida mensual permitido

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.

Como PPoS usa un sistema de un ALGO por un voto, la probabilidad de que estas 100 entidades sean seleccionadas para el comité de votación es cada vez mas alta, aunque no llegan a dominar el comité de validación de bloques, ya que hay miles de otros seleccionados.

**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(per cent) 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).

**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.

Los nodos de red son los que hacen cumplir las reglas de la cadena y aseguran que nadie haga trampa. Por eso, tener una red de nodos robusta, dispersa geográficamente y antifrágil es ideal para la descentralización y la seguridad de la red. Para lograr esto, los costos de funcionamiento de un nodo (hardware, ancho de banda, energía y almacenamiento) deben ser lo más bajos posible. Esto permite que más personas puedan unirse a la red si quieren. Mantener bajos los costos y la inflación estatal asegura que nadie quede excluido y que la red no esté controlada solo por una élite adinerada. Algorand ha decidido no priorizar esto, sino seleccionar a unos pocos privilegiados para mantener la salud de la red.

El objetivo es aumentar la cantidad de transacciones manteniendo una descentralización suficiente. En general, otros esfuerzos de blockchain para aumentar las TPS se han centrado en:

- Acelerar el consenso (permitiendo que los nodos acuerden el orden de las transacciones más rápido)
- Aumentar el tamaño de los bloques (más datos por bloque)
- Disminuir los tiempos de bloque (más bloques por minuto)
- Limitar el conjunto de validadores

Las blockchains diseñadas para un mayor número de TPS, como Algorand o Solana, también enfrentan problemas de centralización. Sin embargo, al igual que los "asesinos de Ethereum" de la era de 2017, sus diseños tampoco son escalables o sostenibles a largo plazo. Algorand ha optado por permitir un mayor número de TPS creando un pequeño conjunto de nodos maestros con permisos, de alto rendimiento pero de alto costo en forma de nodos de retransmisión. Además de la obvia centralización en torno a los nodos con permisos, los nodos de retransmisión requieren mucha potencia informática y costos sustanciales, lo que excluye a la mayoría de las personas del proceso. Además, el costo/carga de almacenar todo el libro de contabilidad está creciendo más rápido que Bitcoin o Ethereum, que tienen una adopción y uso entre 100 y 1,000 veces mayores que ALGO.

## 8 Posibles Soluciones

Estas posibles soluciones pueden ayudar a Algorand a superar sus debilidades actuales y mejorar su sostenibilidad y resistencia en el ecosistema de blockchain a largo plazo.

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

## References


[S. Micali and Jing Chen, 2017] Silvio Micali and Jing Chen. ALGORAND. [Online]. Available: https://algorand.co/technology/research. [Accessed: 17- Oct- 2024].

[S. Micali and Jing Chen, 2019] Silvio Micali and Jing Chen. *Algorand: A secure and efficient distributed ledger.* [Online]. Available: https://algorandtechnologies.com/peer-reviewed-papers/. [Accessed: 17- Oct- 2024].

[Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos and Nickolai Zeldovich, 2017] *Algorand: Scaling Byzantine Agreements for Cryptocurrencies.* [Online]. Available: https://algorandtechnologies.com/peer-reviewed-papers/. [Accessed: 17- Oct- 2024].

[Cosimo Bassi and Naveed Ihsanullah, 2022] Cosimo Bassi and Naveed Ihsanullah. *Proof of Stake Blockchain Efficiency Framework. Algorand, efficient self-sustaining blockchain.* [Online]. Available: https://algorand.co/technology/research. [Accessed: 17- Oct- 2024].

[John Woods, Michele Treccani, John Jannotti and Naveed Ihsanullah, 2023] John Woods, Michele Treccani, John Jannotti and Naveed Ihsanullah. *Algorand Consensus Incentivisation. AN ALGORAND FOUNDATION DISCUSSION PAPER.* [Online]. Available: https://algorand.co/technology/research. [Accessed: 17- Oct- 2024].