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 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.

2.1 ¿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.

3 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.

4 ¿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.

4.1 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.

Format Files

Using LaTEX A LaTEX style file for version 2.09 of LaTEX that implements these instructions has been prepared, as has a BibTEX style file for version 0.99c of BibTEX (not version 0.98i) that implements the citation and reference styles here.

There is also a Word 6.0 template available in RTF-format.

The relevant files are available from the ARAA web server.

`http://www.araa.asn.au/acra`

As the files may be changed to fix bugs, you should ensure that you are using the most recent versions.

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
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 Ihsa
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].