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 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 Layout

Prepare manuscripts two columns to a page, in the manner in which these instructions are printed. The exact dimensions for pages are:

- left and right margins: .75″
- column width: 3.375″
- gap between columns: .25″
- top margin—first page: 1.375″
- top margin—other pages: .75″
- bottom margin: 1.25″
- column height—first page: 6.625″
- column height—other pages: 9″

All measurements assume an 8-1/2 × 11″ page size. For A4-size paper use the given top and left margins, column width, height, and gap and modify the bottom and right margins as necessary.

2.2 Title and Author Information

Center the title on the entire width of the page in a 14-point bold font. Place the names of authors below the title in a 12-point bold font, and affiliations and complete addresses directly below the author names in a 12-point (non-bold) font.

Credit to a sponsoring agency appears in a footnote at the bottom of the left column of the first page. See the example in these instructions.

2.3 Abstract

Place the abstract at the beginning of the first column 3.0″ from the top of the page, unless that does not leave enough room for the title and author information. Use a slightly smaller width than in the body of the paper. Head the abstract with "Abstract" centered above the body of the abstract in a 12-point bold font. The body of the abstract should be in the same font as the body of the paper.

The abstract should be a concise, one-paragraph summary describing the general thesis and conclusion of your paper. A reader should be able to learn the purpose of the paper and the reason for its importance from the abstract. The abstract should be no more than 200 words long.

2.4 Text

The main body of the text immediately follows the abstract. Use 10-point type in a clear, readable font with 1-point leading (10 on 11). For reasons of uniformity, use Computer Modern font if possible. If Computer Modern is unavailable, Times Roman is preferred.

Indent when starting a new paragraph, except after major headings.

2.5 Headings and Sections

When necessary, headings should be used to separate major sections of your paper. (These instructions use many headings to demonstrate their appearance—your paper should have fewer headings.)

Section Headings

Print section headings in 12-point bold type in the style shown in these instructions. Leave a blank space of approximately 10 points above and 4 points below section headings. Number sections with arabic numerals.

Subsection Headings

Print subsection headings in 11-point bold type. Leave a blank space of approximately 8 points above and 3 points below subsection headings. Number subsections with the section number and the subsection number (in arabic numerals) separated by a period.

Subsubsection Headings

Print subsubsection headings in 10-point bold type. Leave a blank space of approximately 6 points above subsubsection headings. Do not number subsubsections.

Special Sections

The acknowledgments section, if included, follows the main body of the text and is headed "Acknowledgments," printed in the same style as a section heading, but without a number. This section includes acknowledgments of help from colleagues, financial support, and permission to publish. Please try to limit acknowledgments to no more than three sentences.

Any appendices follow the acknowledgments (or directly follow the text) and look like sections, except that they are numbered with capital letters instead of arabic numerals.

The references section is headed "References," printed in the same style as a section heading, but without a number. A sample list of references is given at the end of these instructions. Use a consistent format for references, such as provided by BibTEX.

2.6 Citations

Citations within the text should include the author's last name and the year of publication, for example [**?**]. Append lowercase letters to the year in cases of ambiguity. Treat multiple authors as in the following examples: [John Woods, Michele Treccani, John Jannotti and Naveed Ihsanullah, 2023] (for more than two authors) and [**?**] (for two authors). If the author portion of a citation is obvious, omit it, e.g., Levesque [**?**]. Collapse multiple citations as follows: [**?**; **?**].

2.7 Footnotes

Place footnotes at the bottom of the page in a 9-point font.[1] Refer to them with superscript numbers. Separate them from the text by a short line.[2] Avoid footnotes as much as possible; they interrupt the flow of the text.

3 Illustrations

3.1 General Instructions

Place illustrations (figures, drawings, tables, and photographs) throughout the paper at the places where they are first discussed, rather than at the end of the paper. If placed at the bottom or top of a page, illustrations may run across both columns. Securely attach them to the master form with glue stick, spray adhesive, rubber cement, or white tape. Do not use transparent tape as the printing process blurs copy under transparent tape.

Number illustrations sequentially. Use references of the following form: Figure 1, Table 2, etc. Place illustration numbers and captions under illustrations. Leave a margin of 1/4-inch around the area covered by the illustration and caption. Use 9-point type for captions, labels, and other text in illustrations.

1This is how your footnotes should appear. 2Note the line separating these footnotes from the text.

Do not use line-printer printouts or screen-dumps for figures–they will be illegible when printed. Avoid screens or pattern fills as they tend to reproduce poorly.

4 Length of Papers

Submissions must should be within 6 to 10 pages in length.

Acknowledgments

The preparation of these instructions and the LaTEX and BibTEX files that implement them was supported by Schlumberger Palo Alto Research, AT&T Bell Laboratories, and Morgan Kaufmann Publishers.

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`

[1]This is how your footnote should appear.

[2]Note the line seperating these footnotes from the text.

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].