

Analysing Algorand: Possible directions for quantitative analysis

Ivan Malakhov

PRIN NiRvAna project meeting 2024

What is Algorand?

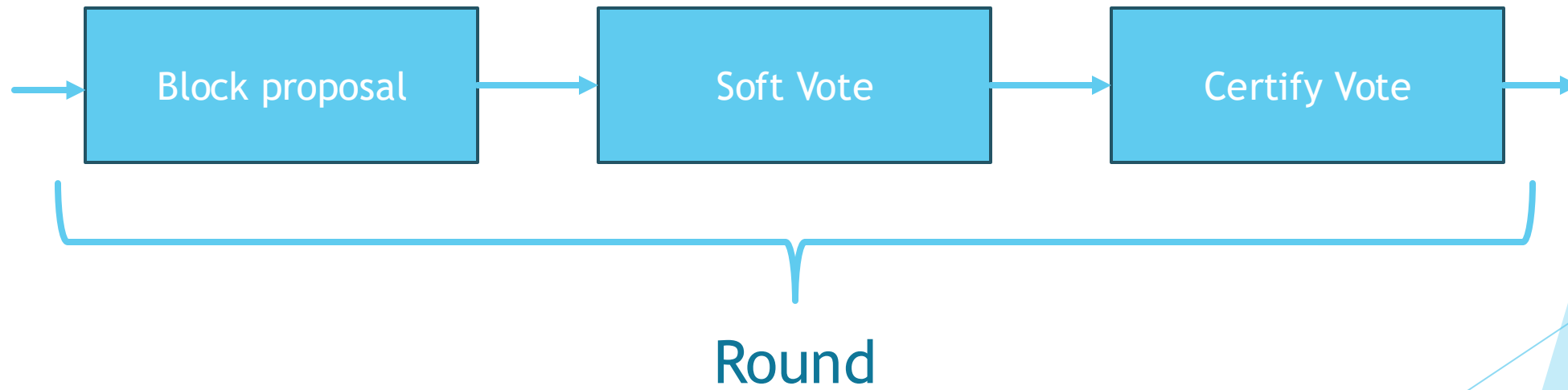
Key features:

- ▶ **Pure PoS consensus**
 - ▶ VRF
 - ▶ Unconditional reward
 - ▶ Forkless
 - ▶ Instant finality
 - ▶ Smart contracts
- ▶ Delegation
 - ▶ FIFO Mempool policy

Verifiable Random Function (VRF)

- ▶ Core mechanism in Algorand's PPoS
- ▶ Elliptic curve
- ▶ Cryptographic sortition
- ▶ Determines randomly if a token is the “winner”

Pure Proof-of-Stake



Pure PoS

- ▶ Scalability
 - ▶ Superfast execution of VRF for the committee
 - ▶ The committee size is apprx. 1000 members
- ▶ Security
 - ▶ Introduction of primary and ephemeral keys
 - ▶ VRF randomness
- ▶ Decentralisation
 - ▶ Total involvement of participants

Forks absence

- ▶ One block to pass the threshold of committee votes
- ▶ 10^{-18} probability of fork
- ▶ All appeared blocks are final (consequence)

Smart Contracts

- ▶ Transaction Execution Approval Language (TEAL)
- ▶ Assembly-like language
- ▶ Struggle to compete with other SC languages

Algorand incentivisation

Standard implementation:

- ▶ All addresses contain a minimum balance or more will receive rewards
- ▶ Determine the *Reward Pool* based on number of blocks in *Reward Period* and fixed per block reward
- ▶ Split the per block reward amount across all token holders based on the amount of stake
- ▶ Block reward depends on effective balance

Algorand incentivisation

Algorand Consensus Incentivisation

AN ALGORAND FOUNDATION DISCUSSION PAPER

John Woods
john@algorand.foundation
john@postquantum.dev

Michele Treccani
michele@algorand.foundation

John Jannotti
jj@algorand.com

Naveed Ihsanullah
naveed@algorand.foundation
naveed@jamsni.com

Version 1.0, 14th December 2023

1 Purpose

The goal of this project is to engineer a native solution at layer 1, modifying the Algorand proto-

Algorand incentivisation

Proposal of Deflating block reward mechanism

$$R(\eta) = (1 - \frac{\eta}{\mathcal{N}})$$

then, adding a normalisation factor:

$$\mathcal{K} = \sum_{\eta=1}^{\mathcal{N}} R(\eta) = (\mathcal{N} - \frac{\mathcal{N}(\mathcal{N}+1)}{2 \times \mathcal{N}})$$

⇒ the payout function is defined as:

$$\mathcal{R}(\eta) = \mathcal{M} \times R(\eta) \times \frac{1}{\mathcal{K}}$$

linear

$$R'(\eta) = e^{-\rho \frac{\eta}{\mathcal{N}}}$$

then, adding a normalisation factor:

$$\mathcal{K} = \sum_{\eta=1}^{\mathcal{N}} R'(\eta) = \frac{1 - e^{-\rho}}{1 - e^{-\frac{\rho}{\mathcal{N}}}}$$

⇒ the payout function is defined as:

$$\mathcal{R}'(\eta) = \mathcal{M} \times e^{-\rho \frac{\eta}{\mathcal{N}}} \frac{1}{\mathcal{K}}$$

exponential

Where η : number of a starting block

- \mathcal{M} : Total units for incentive (e.g., 200 million Algo)
- \mathcal{B} : Block-time (e.g., 3 seconds)
- \mathcal{T} : Total duration for the payout, expressed in seconds (e.g., 3 years)
- \mathcal{N} : Total number of blocks over the payout period
- ρ : Rate of decay

Algorand vulnerabilities

Attack vectors and their potential mitigations:

- ▶ Absenteeism -> Suspension from the stake
- ▶ Pooling -> Participation Key expiration
- ▶ Protocol deviation -> “negligible”?

Algorand analysis

allo'

HOME

EXPLORE

RESOURCES

MY BOOKMARKS

Alerts
Monitor on-chain events and consensus participation

Account
Manage your addresses and settings

allo' ^{Hi!}

All of Algorand. For everyone.

algoscan

Thank you for using algoscan.

We've shutdown after 2.5 years due to lack of funding.

Algoscan shutdown August 31st, 2023. [Full Statement Here](#)

algoscan

A Blockchain Explorer and Analytics Platform built on Algorand. (v2.0.0)

SOCIAL

Dappflow

HomeAccountsTransactionsAssetsApplicationsMemPool

Algonode mainnet

Dashboard

Explorer

Asset Manager

App Manager

Beaker Studio

ABI Studio

Node Manager

KMD Portal

Developer API

Dev Wallets

Composer

Advanced search

Latest block

39,523,499

Total transactions

1,919,841,688

Genesis ID

mainnet-v1.0

Build version

3.24.0

Latest Blocks

#39523499

appl=7, pay=32, axfer=4

6 seconds ago

43 Transactions

#39523498

appl=9, pay=79, axfer=15

9 seconds ago

103 Transactions

Latest Transactions

PWJ3M3WT422JLFROGTUIGFGEMUUGEHEADH2H4YI6...

App call

From : WARN666I8ITOTBIFMYOQYDAT2...

To : Application: 1284326447

N2ZQOMLDKVG6YFA7ALGKIYDTU6RYYSDFUJA3KSKT4...

Roundment

pera Explorer MAINNET

Search by ID, name or address

Download Pera Wallet

Transactions

Show live updates

Transaction ID	Block	From	To	Amount	Type	Age
43NYN7LVL...	39523533	ZW3I...W754	IAZH...BZIE	0.00 Planets	Asset Transfer	0 minutes
P4AIZEQPF...	39523533	ZW3I...W754	T72A...MJOU	0.00 Planets	Asset Transfer	0 minutes
YZNMYLMNV...	39523533	ZW3I...W754	2Y7M...YGV	0.00 Planets	Asset Transfer	0 minutes
F5ZSMNP65...	39523533	7BYZ...AAJM	DSOP...K6S4	0.00 FRY	Asset Transfer	0 minutes
SRQZFRWQ2...	39523533	YW6B...RKAY	YW6B...RKAY	0.00 HX	Asset Transfer	0 minutes
O3F4RIA5T...	39523533	JRZR...7544	DSOP...K6S4	0.00 FRY	Asset Transfer	0 minutes

Conclusion

Promising PoS-based blockchain with solid academic background

- ▶ Lacks substantial incentivisation mechanism
- ▶ Validators' absenteeism
- ▶ Pooling and delegation
- ▶ Protocol Deviation