Algorand
Blockchain Protocol
–
An Overview

By:

Ayse Karaman, Ph. D.

December 2017

Contents

- Algorand as "*a*" blockchain protocol
  External/environmental characteristics
  - PoS, permissionless, decentralized
  - The Adversary
  - Ledger structure
  - Byzantium consensus
- Algorand as *"the"* blockchain protocol
  Security structure, internal characteristics
  - Byzantium consensus
  - Block signing – Rounds, Role players
  - Round duration
  - Cryptographic sortition
  - Player replaceability
  - The keys
  - Forks?

Algorand As "*A*" Blockchain Protocol

Algorand

Brainchild of ***Silvio Micali***
https://people.csail.mit.edu/silvio/

A fast, binary Byzantium agreement protocol
to reach consensus on transactions

- Proof of Stake
- Permissionless
- Decentralized – fully
- Cryptographic

PoS – Proof-of-Stake

Role players in block signing

- A set of Algorand users to certify the blocks
- Which users?
  - Stakeholders
  - Selected randomly – cryptographic sortition
- The stake

  Algorand coins currently at hand
  - Chances of taking a role is directly proportional, *not* exponential to the stake
  - The only means a user can influence his chances of role assignment
- Algorand coins are not on hold during selection
- 2/3+ of stakes in honest hands

Permissionless

- Each digital key is an Algorand user
  - Public-key component, *PK* – the user-ID
  - How to join?

    Appear on ledger as a recipient of Algorand coins
- Private

  No forced mapping between Algorand user and real-life user
  - Can hold multiple digital keys
  - Doesn't have to reveal real-life ID
- Anyone can join anytime

  No approval necessary
- User has full control of his secret key

  No central authority

Decentralized

Fully decentralized

- Nodes fully homogeneous in their functionality
- P2P gossip – underlying message delivery
- Ledger look-up – the only external reference
- Each user listens to the network and acts on protocol rules using its local functionality
  - No reliance on intermediary nodes or external processes
  - No super- or seed-nodes to organize the Algorand network
  - No servers of any kind, not even a universal time
    - Clocks should tick at same intervals on all nodes – Algorand's only time-wise requirement

The Adversary

A powerful one

- **Can**
  - Corrupt users instantly
  - Coordinate bots towards a specific action
  - See all messages instantly

    Anyone can, but the assumed adversary is least effected by propagation delay
  - Conceal itself till it acts up

    No way to know who the malicious users are till their malicious act
- **Can Not**
  - Corrupt 1/3 of users
  - Forge signatures, break hashes – no exponential computing power
  - Interfere with messages between honest users

The Ledger

Much like the Bitcoin ledger

- Blockchain
  - Temporal sequence of approved blocks
  - Linked by hash-pointers
- Block structure
  - Set of valid transactions
    - Unordered set
    - Valid by transactions on all prior blocks
  - Hash of previous block – the *chain*
  - Also includes round#
    Algorand operational purposes – no effect on use of Ledger
  - Also includes Q_r – random seed
    ditto
  - Certificate – signatures of 2/3+ of verifiers who worked on it
- Query by user-ID
  The public key
  - PoS – look up stakes for role verification

The Ledger – Cont'd

- Immutable
  In order to change a block, change all blocks after it and forge all signatures certifying them
  - Hash-pointer – block content changed
  - Centuries of computing
- "Posted on the sky"
  - Each new block and its credentials circulated for everyone to see
  - Can be viewed by anyone, anytime
    No restrictions, no control
- Fully decoupled from the protocol
  No imposed/assumed structure beyond a blockchain with the content
- Fast queries – ledger look-up time
  - Can be critical early in the block-signing round
    The "seed" to select the next committees is on latest block
  - More critical than for many other blockchain protocols
    Looked-up by a different committee at every step
  - Time boundary – Algorand "exits" on certain time limits