Alternative Consensus 1

Algorand: Scaling Byzantine Agreements for Cryptocurrencies

Algorand is using new Byzantine Agreement. To scale it uses Verifiable Random Function to give people possibility to check if they are selected in next BA. Faster 125x than bitcoin, can be well scaled. Allow participant replacing.

Three main problems: Sybil attacks | Weighted users,Scalability (BA dont operate millions), resilitent for ddos attacks. Consensus by commettee, Cryptographic sortition (BA chooses commitee privatly and user can check if he is chosen using VRF function), Participant replacement(just once).

BA* avoids forks and centralized authority.

Saefty goal - all agree on one thansaction, liveness goal- - the system continue to grow every one minute. 2/3 monetary value to honest nodes. Strong synch assumption - liveness, safety - low synch assumption.

Gossip protocol- randomly selected weighted peers, messages are signed. User executes sortition and if he is selected he distribute block to other peers.BA* ensures agreement on one block. Final consensus - avoid forks, tentantive agreement - users can see different versions due network conditions. Under strong synch agreement on 4 steps.

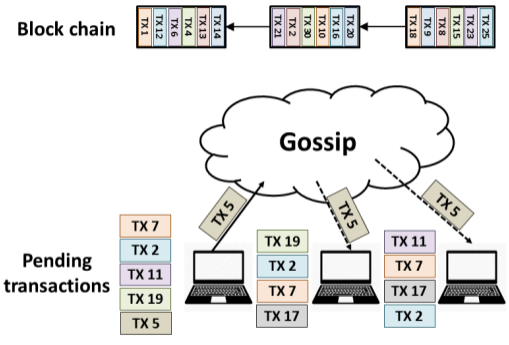


Figure 1: An overview of transaction flow in Algorand.

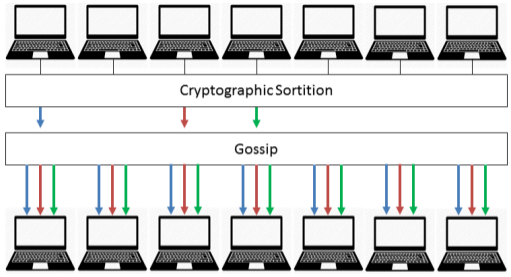


Figure 2: An overview of one step of *BA⋆*. To simplify the figure, each user is shown twice: once at the top of the diagram and once at the bottom. Each arrow color indicates a message from a particular user.

VRF return the proof to verify withour private key. Random seed for selection every round(based on previous), to prevent attack algorand can look back on b amount of blocks (if hacker blocked the new seed and controll network using hash based seed). Weak synch - there was a moment than network worked great

Threshold - how many users selected to propose.Block proposers prioritize.First gossip small messages, after sending a block. User waits to ensure that he received the highest priority.
BA contains of 2 phases: Reduction (block or empty block), Binary agreement (final agreement). Committee voting (need 2/3 of votes). The common coin is a random value based on VRF hashes that pushes users toward one decision after multiple steps (using last bit of vrf hash).⟨hash,π⟩=VRFsk(seed ∣∣ role)

If block is not valid - empty. Fork recovery protocol (Detect 2 chains → Single longest fork that includes all blocks → Constensus using BA). Storage shard across users. Randomized users graph. Communication cost constant. Validation before passing a block. Each block has a cerifiifcate (no need to verify txs)

Blockene: A High-throughput Blockchain Over Mobile Devices

Blockene- lightweigt blockchain to run on mobile entities. Split trust design. Uses low energy, network and storage. Two types of nodes: citizens and politicians (server). For security: replicated verifiable read (read from multiple server and verify using proof) and sample-based Merkel Tree(citizens verify small part of blockchain and not all). Uses Prioritize gossip mechanism (priority to the important info), predeclared commit (make and record decision before making it).

Around 1045 transactions per second.

Citizens validate transactions before sending them in block (get balances and history from politicians). Random committies validates each block.

Citizen attacks - sybil attacks (each user - unique device), bribe cannot be done (limitation for phone notifications). Politicians attacks - 80% dishonest. Covert attack - stainless,split-view, drop, dos and sybil attack.

Around 200 politicians. Choice of committies using VRF for 10 next blocks (2000 citizens). 5 rounds to have a consensus. No forks are possible. Incremental

validation- make a local copy every 10 blocks. 40 blocks- cool off period.

Optimizations : prioritized gossips(handshake with lackins txs, more tx → more priority), sampling based merkle tree (randomly verify some art and not all)

Proof of safety(consistent state), liveness(not stale) and fairnes (all included)