Algorand™
Protocol Overview

The Algorand blockchain uses a decentralized Byzantine agreement protocol that uses pure proof of stake (PPOS). This means that it can tolerate malicious users, achieving consensus without a central authority, as long as a supermajority of the stake is in non-malicious hands. This protocol is very fast and requires minimal computational power per node, giving it the ability to finalize transactions efficiently.

Before getting into detail on the protocol, we discuss two functional concepts that Algorand makes use of.

VERIFIABLE RANDOM FUNCTION

Recently we released the source code for our implementation of a Verifiable Random Function (VRF). The VRF takes a secret key and a value and produces a pseudorandom output, with a proof that anyone can use to verify the result. The VRF functions similar to a lottery and is used to choose leaders to propose a block and committee members to vote on a block. This VRF output, when executed for an account, is used to sample from a binomial distribution to emulate a call for every Algo in a user's account. The more Algos in an account, the better chance the account has of winning – it's as if every Algo in an account gets its own lottery. This method ensures that a user does not gain any advantage by creating multiple accounts.

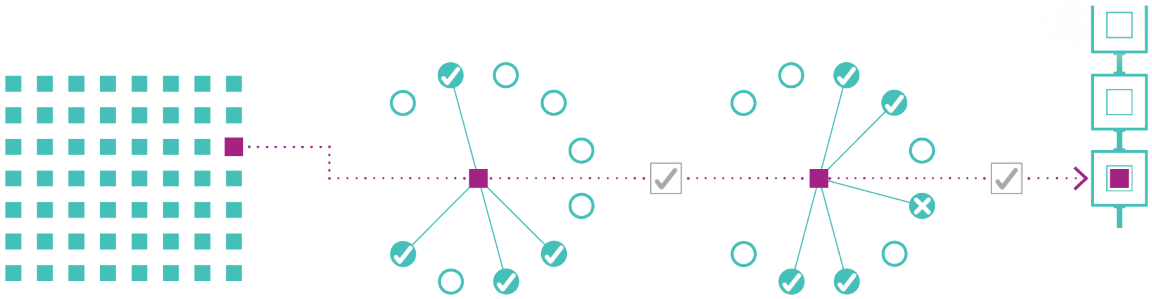
PARTICIPATION KEYS

A user account must be online to participate in the consensus protocol. However, to reduce exposure, online users do not use their spending keys (i.e., the keys they use to sign transactions) for consensus. Instead, a user must generate and register a specialized participation key before going online. With this key, an online account can participate in proposing and confirming blocks. A participation key expires after a certain number of rounds, after which it is removed and a new participation key must be generated to continue participating. Using participation keys ensures that a user's money is secure even if their participating node is compromised.

THE ALGORAND CONSENSUS PROTOCOL

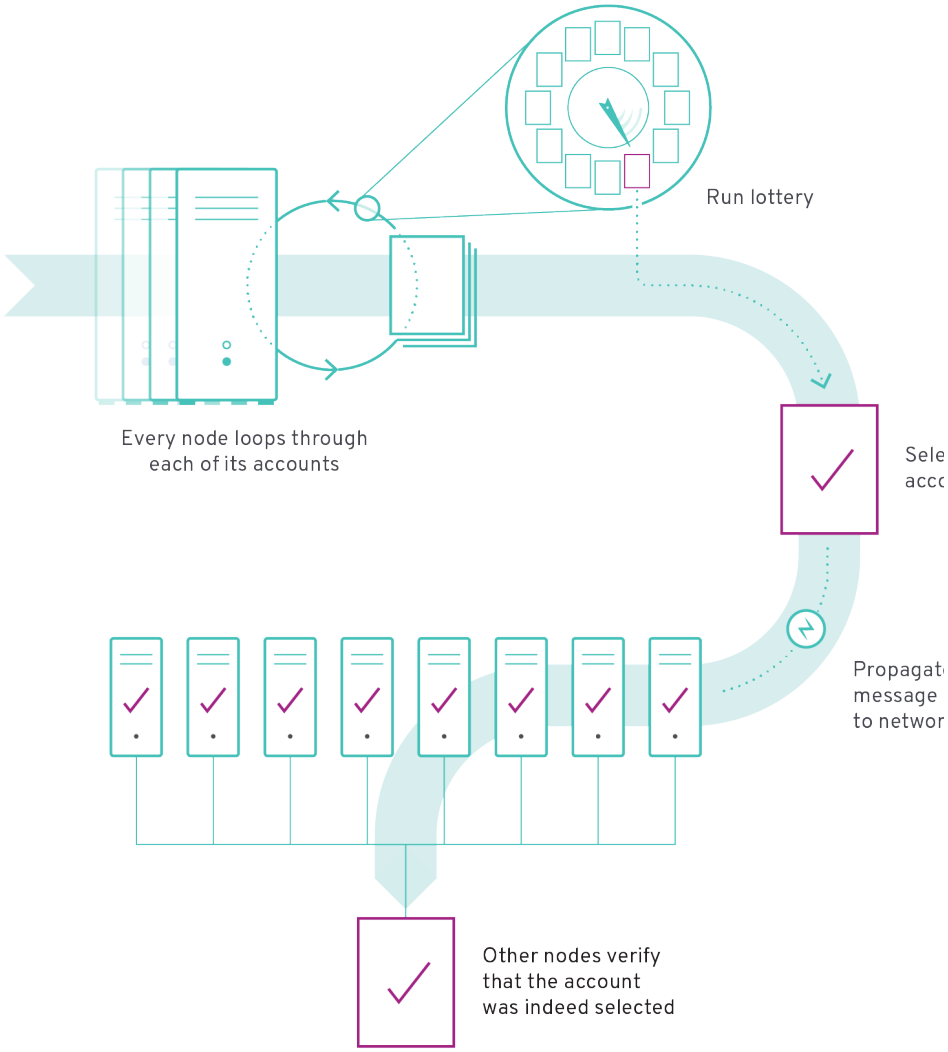
Consensus refers to the way blocks are selected and written to the blockchain. Algorand uses the VRF described above to select accounts to propose blocks for a given round. When a block is proposed to the blockchain, a committee of voters is selected to vote on the block proposal. If a super majority of the votes are from honest participants, the block can be certified. What makes this algorithm a Pure Proof of Stake is the fact that when committees are chosen they are based on the number of Algos an account has. Committees are made up of pseudorandomly selected accounts with voting power dependent on their online stake. Therefore, it is feasible and probable that some accounts will have a higher number of votes than other members on the committee. Using randomly selected committees allows the protocol to still be performant while allowing anyone in the network to participate.

Consensus requires three steps to propose, confirm and write the block to the blockchain. These steps are: 1) propose, 2) soft vote and 3) certify vote. Each is described below, assuming the ideal case when there are no malicious nodes and the network is not partitioned (i.e., none of the network is down due to technical issues or from DOS attacks). Note that all messages are cryptographically signed and authenticated with the VRF in these steps.



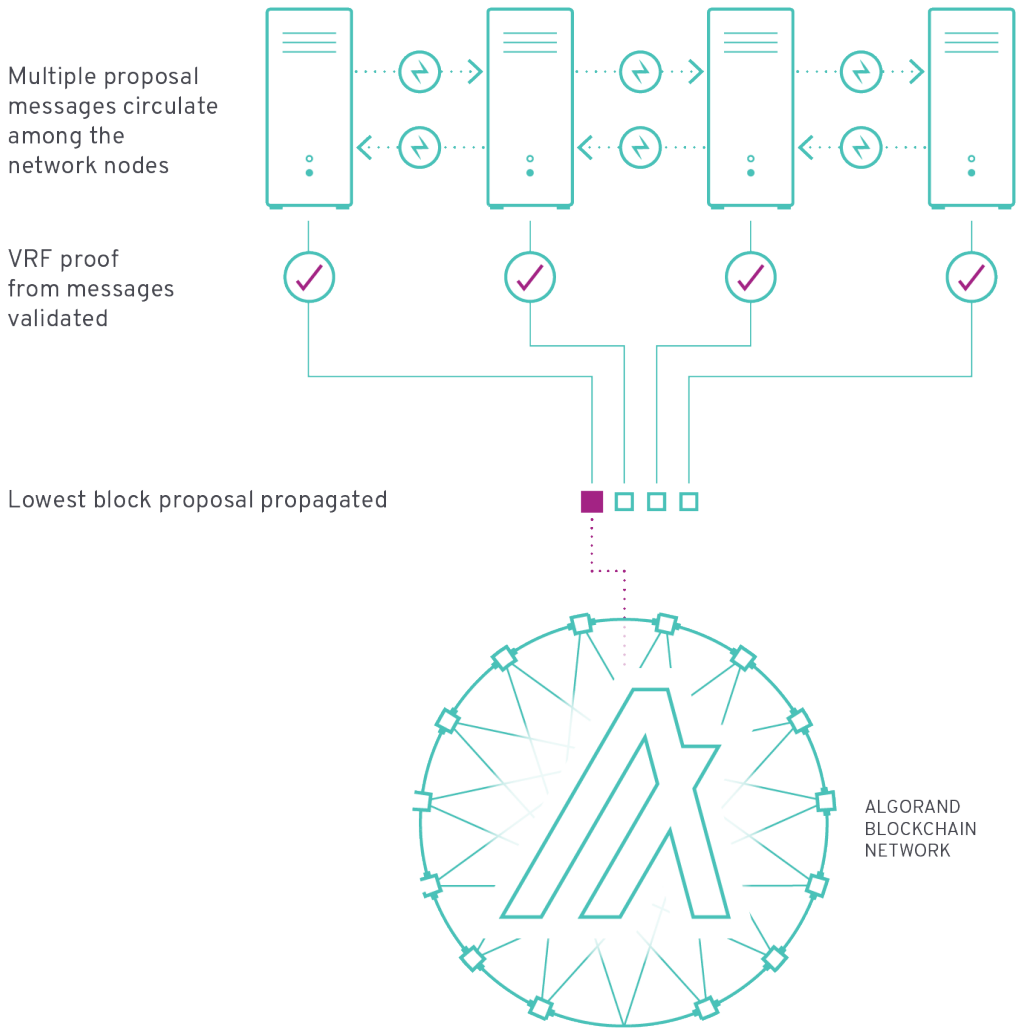
BLOCK PROPOSAL

In the block proposal phase, accounts are selected to propose new blocks to the network. This phase starts with every node in the network looping through each of the accounts that it manages, and for each account that is online and participating, running Algorand's VRF to determine if the account is selected to propose the block. The VRF acts similar to a weighted lottery where the number of Algos that the account has participating online affects the account's chance of being selected. Once an account is selected by the VRF, the node propagates the proposed block along with the VRF output, which proves that the account is a valid proposer. We then move from the propose step to the soft vote step.

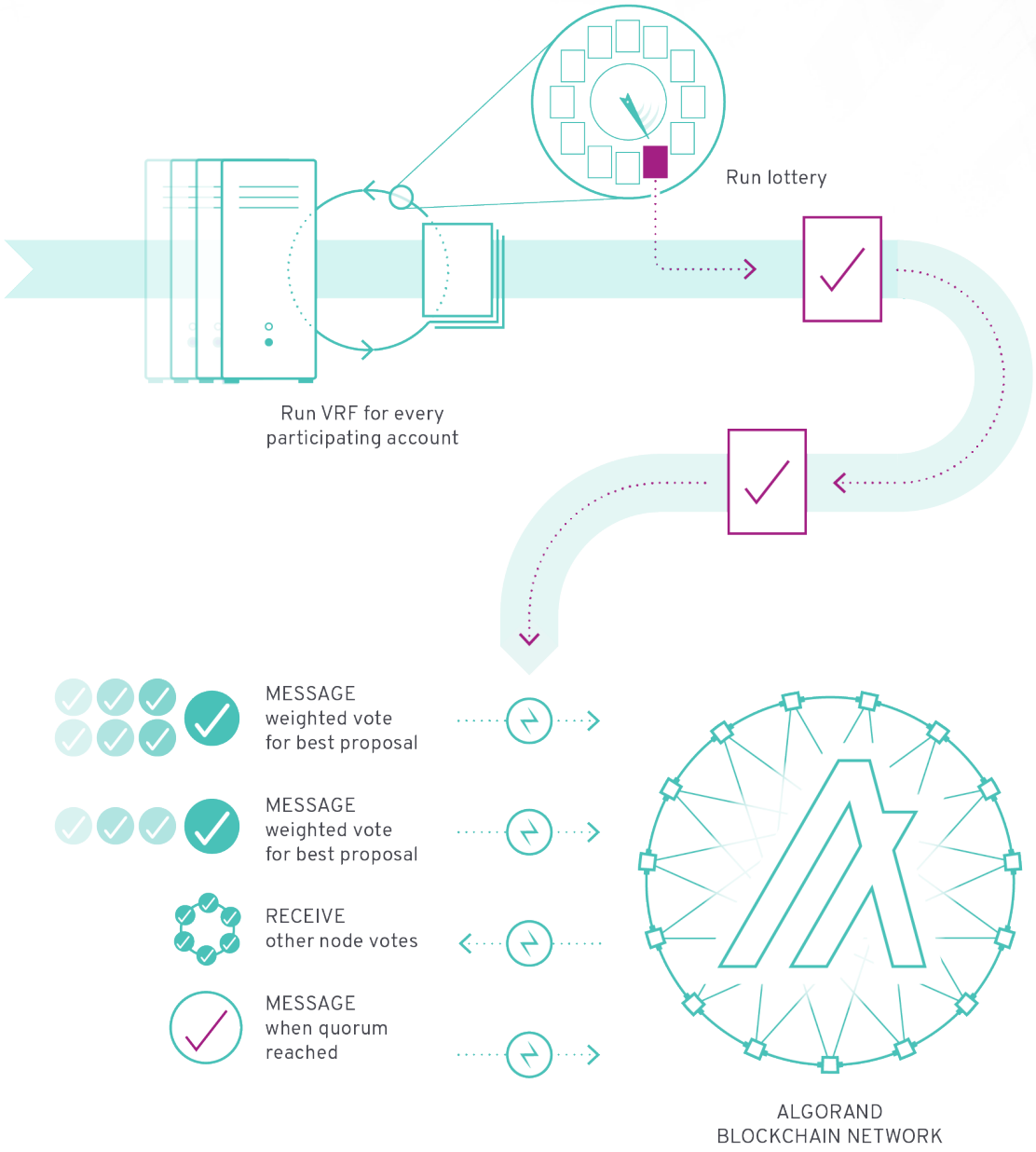


SOFT VOTE

The purpose of this phase is to filter the number of proposals down to one, guaranteeing that only one Block gets certified. Each node in the network will get many proposal messages from other nodes. Each node will validate the VRF proof of these messages. Next, the node will compare the hash from each validated winner's VRF proof to determine which is the lowest and will only propagate the block proposal with the lowest VRF hash. This process continues until the timeout occurs for this step.



Each node will then run the VRF for every participating account it manages to see if they have been chosen to participate in the soft vote committee. If any account is chosen it will have a weighted vote based on the number of Algos the account has, and these votes will be propagated to the network. These votes will be for the lowest VRF block proposal calculated at the timeout and will be sent out to the other nodes along with the VRF Proof.

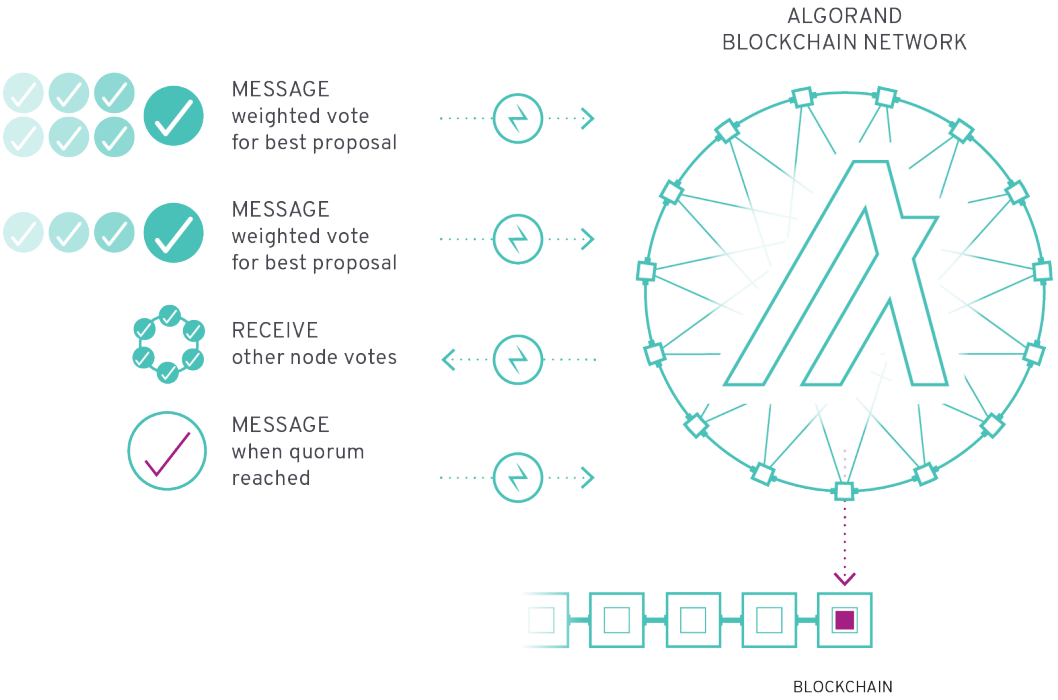


A new committee is selected for every step in the process and each step has a different committee size. This committee size is quantified in votes, not accounts. A quorum of votes is needed to move to the next step and must be a certain percentage of the expected committee size. These votes will be received from other nodes on the network and each node will validate the committee membership VRF proof before adding to the vote tally. Once a quorum is reached for the soft vote the process moves to the certify vote step

CERTIFY VOTE

A new committee checks the block proposal that was voted on in the Soft Vote stage for overspending, double-spending, or any other problems. If valid, the new committee votes again to certify the block. This is done in a similar manner as the Soft Vote where each node iterates through its managed accounts to select a committee and to send votes. These votes are collected and validated by each node until a quorum is reached, triggering an end to the round and prompting the node to create a certificate for the block and write it to the ledger. At that point, a new round is initiated and the process starts over.

If a quorum is not reached in a certifying committee vote by a certain timeout then the network will enter recovery mode.



RECOVERY

If the network does stall, either from network outages or malicious behavior, the nodes go into recovery mode, waiting for recover messages. Individual nodes will send these messages to signal to the network that it should either continue processing the last known block proposal or to propose a new block. When a quorum of votes is received for either one of these messages, the system will revert to normal operation. In the case of malicious behavior, the protocol may select a new leader. In the case of network outage, the current block will continue to be processed or a new block might be proposed.

SAFETY VS. LIVENESS

Algorand optimizes two major attributes of the network and these are safety and liveness. Safety means at most one block is certified and written to the chain in a given round, preventing forks. Liveness means at least one block is eventually written to the blockchain. As discussed previously, the protocol does allow stalls from malicious behavior or network issues, and we allow this because safety is prioritized over liveness. The recovery mode allows the network to continue processing after the stalling problem passes.