Kasper Borgbjerg
kasperib@uio.no

Blockchain Alternative consensus 1

Algorand is a layer one blockchain technology in which its developer team and the blockchain technology itself, are highly focused on scalability; and at the same time mitigating the negative effects between speed, security, and decentralization.
Moreover, Algorand is a permissionless blockchain that is targeted towards defi and dapps (similar to Ethereum). The consensus protocol of the network is regarded as Pure Proof of stake (PPOS) where essentially every user on the network can be chosen to propose blocks and vote for block proposals. The likelihood that a node will be chosen for validation is proportional to the amount staked from that account (conventional pk, sk mapping). The lucky nodes that are chosen by the raffle will be assorted in committees, that work together to delegate the consensus labor. The labor is comprised of hashing as in other networks, in this specific case, however, the algorand network has designed a generic function for this, called the verifiable random function (VRF). Conforming to a Byzantine agreement consensus, the ethos of the network relies on the majority of the nodes to be honest in order to provide the security and liveness properties for the network (2/3 of the nodes are honest).
User growth on the network has a minimal effect on the latency of the network, and this has been described to be almost insignificant when scaling from 5000 to 50000 users (Gilad Y et.al. 2017). Also, the throughput of the network is designed to broadcast blocks of different sizes, from 512KB to 10MB (as measured under testing conditions). This increase in block size has seen positive effects on the throughput of the network without bringing too negative effects on the latency.

Kasper Borgbjerg
kasperib@uio.no

References:

Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. *Algorand: Scaling Byzantine Agreements for Cryptocurrencies*. ACM; 2017:51–68. doi:10.1145/3132747.3132757