A Review of ‘Algorand: Scaling Byzantine Agreements for Cryptocurrencies’

Prashanth R Duggirala

Summary

Paper by Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos and Nickolai Zeldovich, 2017

Algorand is a new cryptocurrency system that can confirm transactions with latency on the order of a minute while providing good scalability. One of the main features of Algorand is its low probability of forking, unlike in many other blockchains, users are very unlikely to see different versions of the ledger at any time. The paper talks about the limitations of the current cryptocurrencies that are based on the proof of work concept, it talks about scalability issues, transaction latency and also stresses on the wastefulness of resources to demonstrate proof of work and forking and how a user must wait for a longer time to finally confirm that his transaction is still in the blockchain because of the multiple forks forming. The paper talks about how not only proof of work, but a user’s stake, i.e. how much currency they possess is a reasonable way to prove honesty because it is much more efficient to prove. Algorand assumes that at least two-thirds of all coins are held by honest users, it is called honest majority of coins, an honest user is one who follows the Algorand protocol exactly as prescribed. Algorand also relies on assumptions about the connectivity of participants, to ensure that the network cannot get out of sync due to users failing to participate in the protocol for long intervals of time. The weak synchrony assumption of algorand is that an adversary might completely control the network connectivity for a bounded period of time, but the network must always return to being able to send and receive messages from most honest users within a time interval, also called strong synchrony, again for long enough to recover. The primary goals of Algorand are improving scalability, increasing transaction throughput with increasing number of nodes, decreasing transaction latency and making more efficient use of computational resources by avoiding Proof of Work.

The core of Algorand is a new Byzantine agreement protocol called BA★. Participants in BA★ are randomly selected based on a proof-of-stake mechanism that relies on a concept called cryptographic sortition. Every user is assigned a private key and a secret key. The system also includes a log of cryptographic transactions stored as a chain of blocks, and a gossip protocol for broadcasting transactions where every user collects a block of pending transactions that they hear about. Users are elected to a committee with probability proportional to their stake in the system, i.e. how many coins they own. Each member of the committee proposes a block, and the committee attempts to come to a consensus about which proposed block to validate. When multiple blocks are proposed, the committee is to choose the block from the highest weight user. BA★ is used to reach consensus on a block (either a block containing correct transactions, or an empty block). The execution of BA★ consists of two phases. In the first phase, BA★ reduces the problem of agreeing on a block to agreement on one of two options. In the second phase, it reaches agreement on one of these options: either agreeing on a proposed block, or agreeing on an empty block. During this protocol, new committees are chosen after each voting step, and each time, the votes are broadcast to all users. This creates a more scalable system than Proof of Work based systems, since the transaction confirmations are much more efficient.

Strong points

1. Algorand overcomes the various limitations faced by other popular cryptocurrencies which are based on Proof of Work based consensus like wastefulness of resources, time taken to commit a new block and scalability issues.

2. Algorand achieves true decentralization as it uses proof of stake consensus rather than proof of work where there exist individuals or corporations that control enormous compute power.

3. Using the byzantine agreement protocol, algorand commits new blocks with a fraction of time compared to other cryptocurrencies which ensures quicker finality of transactions.

Weak points and comments

1. This protocol assumes that at least two thirds of all the coins are owned by honest users. There might be less chance for a users with most coins be malicious but the possibility can not be overlooked so this is still a weakness.

2. The gossip protocol itself could be vulnerable to attacks, and its security properties have not been discussed comprehensively but I believe they should.

3. A security analysis research paper on algorand shows that it is possible to slow down the message validation process on honest nodes, which eventually forces them to choose default values on the consensus; leaving the targeted nodes behind in the chain as compared to the non-attacked nodes.

References:

1. "Algorand: A Better Distributed Ledger," with Silvio Micali
2. https://inst.eecs.berkeley.edu/~cs261/fa18/Algorand.pdf
3. Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages