Alternative Consensus

According to the long wait requirement for confirmation of a transaction in Bitcoin, we are encountering a trade-off between latency and confidence in a transaction. Algorand is a new cryptocurrency designed for confirming transactions on the order of one minute. BA* is a Byzantine agreement protocol that Algorand utilize it to reach consensus on a new block with low latency and without the possibility of forks. BA* uses verifiable random functions to randomly select users in a private and non-interactive way.

Algorand solves three main challenges. First, it avoids Sybil attacks, where an adversary creates many pseudonyms to affect the Byzantine agreement protocol. For this purpose, Algorand assigns a weight to each user based on the money in their account. Therefore, as long as more than 2/3 of the money is owned by honest users Algorand can avoid forks and double-spending. Second, Algorand scales to millions of users by the help of BA*. Scalability is achieved by choosing a small set of representatives randomly selected from the total set of users called a committee to run each step of its protocol. The committee users are chosen randomly based on the user's weights. At the end, Algorand avoids denial of service attacks and maintain operation even if an adversary disconnects some of the users. The reason that BA* selects committee members in a private and non-interactive way is to avoid adversary from targeting committee members. Since membership selection is non-interactive, an adversary does not know which user to target until the user starts negotiating in BA*. In order to prevent an attack to a committee member once that member sends a message in BA*, committee members speak just once. Based on this algorithm, all users equally participate and new committee members are elected for each step of the Byzantine agreement protocol.

Bitcoin-NG (Next Generation) is another blockchain protocol designed to solve the scalability limits of Bitcoin about the trade off between throughput and latency. Bitcoin-NG is a Byzantine fault tolerant blockchain protocol which is robust to extreme churn and scales optimally. Performance improvement of Bitcoin-NG is the result of decoupling Bitcoin's blockchain operation into leader election and transaction serialization. Bitcoin-NG divides time into epochs and each epoch has a single leader. This leader is elected randomly and infrequently. The responsibility of the leader is to serialize transactions unilaterally and generate blocks until a new leader is chosen. The protocol introduces two types of blocks. Key blocks are for leader election and microblocks contain the ledger entries. Bitcoin also had leader election for generating blocks, but in Bitcoin there were a long system freeze during the time between leader elections. However, Bitcoin-NG ensures that the system is able to continually process transactions by its leader election mechanism.