Alternative Consensus 2

Tim Sigl

Bitcoin-NG decouples Bitcoin’s blockchain operation into two distinct operations. First a leader is elected and afterwards the transactions serialized. Time is divided into epochs with a single leader for each epoch. Two types of blocks exist in Bitcoin-NG. The key blocks are used for leader election and the microblock holds the ledger entities. A key block can be mined like in Bitcoin but contains an additional public key. The node able to mint the key block becomes the leader for the current epoch and can generate microblocks. Miners are incentivized by the reward for a minted key block and the ledger entries that carry a feed that is split between the current and the next leader. Because of the fast production time of micro blocks it may happen that the next leader did not hear about all the blocks yet. Blocks in the short fork are orphaned. Micro blocks do not require any mining. Double spends can be invalidated by poison transactions. One key block is generated in 100 seconds. Even with a high frequency of micro blocks, forks stay rare. Block size in Bitcoin-NG can be increased without suffering under fairness issues or mining power utilization degradation. Bitcoin-NG improves the scalability to the point where the bottleneck is the network bandwidth and the node's individual power.
Blockene is a novel split-trust design based on delegating storage and gossip to untrusted nodes. Nodes can be run on mobile phones costing only 60MB of data per day and only a few hundreds MBs total storage. The battery drain on a mobile is 3% extra per day extra. The two kinds of nods are Citizens nodes which run on a smartphone and have voting power. Politician nodes run on servers and are untrusted. Only 20% of all politician nodes have to be trusted. To find an honest politician to read the data from, citizens read from multiple politicians. Like in Algorand a random committee of 2000 citizens is chosen to run the consensus for each block. Unlike in Algorand the committee is announced before their participation. Sybil attacks are prevented by trusted hardware on the smartphone. Citizens do not store blockchain, they only store a list of valid citizens. TPS degrades by 75% if 25% and 80% of politicians are dishonest.
Different membership selections can be employed to select a committee for consensus. Proof-of-Work addresses the problem of Sybil attacks by requiring nodes to prove that they have done some work and spend electricity in forms of hardware. There are often reward structures on finding blocks. The issue is the high resource consumption. One assumption for PoW to work is that the majority of hashing power is in the hands of honest nodes. There are two variants of PoW that use the CPU or are memory-bound. Proof-of-Reputation is an extension of PoW. It counts the total valid work a miner has contributed over the entire period of time. So there is no instant reputation through powerful hardware. Reputation drops to zero when an attack is detected. In Proof-of-Stake consensus participants are required to deposit something of value at stake. Often the deposit will be taken away if the node is acting maliciously. PoS is environmentally friendlier than PoW and has an improved throughput. Voting power is proportional to the stake nodes hold. The issue of “Nothing at stake” describes a situation where a stakeholder votes for all possible proposals with the same stake to lose the vote by any chance. There are mechanisms in place to punish that kind of behavior. Algorands VRF selects a random subset of nodes. Only the nodes selected for the next consensus step know that they are selected, similarly works Ouroboros. In delegated PoS nodes with stake for other nodes to become their delegates. In Proof-of-Burn,

blocks are created by burning a specific amount of coins. In Proof-of-Authority only trusted nodes are able to mint new blocks. This approach centralizes the blockchain and is mainly used for testing purposes. Two algorithms implementing PoA are Aura and Clique. Proof-of-Capacity utilizes hardware storage. Opposite to PoW are hardware resources not wasted but used for storing the blockchain in a sharded format. The issue is that space can easily be rented from cloud providers. TEE-based consensus algorithms rely on trusted execution environments found on chips from different hardware manufacturers. The chips can calculate a random next leader. In Proof-of-Location physically close peers validate the location of other peers. This method is mainly used in IoT applications and has the issue of location spoofing.