Kasper Borgbjerg
kasperib@uio.no

Blockchain Alternative consensus 2

Bitcoin-ng is a scalable blockchain protocol and enhancement to the original bitcoin protocol, that promises higher throughput and lower latency. The metrics that determine the network throughput are the size of the blocks and the block interval in which these blocks are mined. Increasing the blocksize of the bitcoin network and keeping the interval rate for block proposal would allow for more transactions, but then also lead to consensus latency (as bigger blocks disseminate slower through the network). Increasing the block interval proposal time would also boost the throughput of the network but suffer from the same downsides of higher rates of forks. Bitcoin-NG proposes an alternative architecture to bitcoin in which the network is comprised of two sets of blocks, key blocks and micro blocks. Key blocks are the only block type necessary to mine (performing POW hashing to hit below target) where microblocks contain the transactions transmitted. Furthermore, the network is split up into epochs of time, where each epoch has an elected leader. The leader is chosen on behalf of the key block that it must produce. The elected leader is responsible for producing the blocks in the epoch in which it is sovereign.

Back to the blocks. The microblocks are cryptographically tied to the key block of that epoch. The mining rewards are divided in a 40/60% distribution, where the leader of the epoch receives the 40% of the reward while the subsequent leader received the 60% (Eyal et.al. 2016). The miners are motivated to include the transactions in their microblocks, extend the heavies chain, and extend the longest chain. The microblocks carry no weight to prevent adversaries to conduct selfish mining (where they would work on several blocks at the same time and propose them in a short period to change the working branch).

Kasper Borgbjerg
kasperib@uio.no

References:

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). {Bitcoin-NG}: A Scalable Blockchain Protocol. In *13th USENIX symposium on networked systems design and implementation (NSDI 16)* (pp. 45-59).