Alternative Consensus 2

Lars Erik Wik

March 29, 2022

Summary

With the increasing popularity of cryptographic currencies, the need for scalable blockchain ledgers increase. The bottleneck in blockchain scalability resides in the consensus algorithms. Considering the well known Nakamoto consensus protocol, used in many of today's blockchains, we can see that it significantly suffers from high latency and low throughput. Some blockchains attempt to improve these properties by tweaking parameters like block size and block interval, but this comes with the cost of stability. Instead we need alternative consensus algorithms.

Ittay Eyal et al. [1] proposes Bitcoin-NG. In Bitcoin-NG time is divided into epochs. For each epoch a leader is elected by mining a *key block* using Proof-of-Work. Once elected, the leader is allowed to generate *micro blocks* containing transactions. The leader is incentivised to create *micro blocks*, as the leader will receive 40% of the transaction fees, while other miners are incentivised to participate based on the fact that they may receive 60% of the transaction fees in case they're elected as the next leader.

Sambhav Satija et al. [3] proposes Blockene. In Blockene participation is divided into *Citizens* and *Politicians*. *Citizens* run on smartphones and have voting power, while *Politicians* run on servers and do the heavy lifting. The consensus algorithm run in the *citizens* is inspired by Algorand, in that It randomly chooses a committee of N nodes using a Verifiable Random Function. The committee then runs PBFT to achieve consensus. *Citizens* are identified using the trusted hardware TEE available in most smartphones.

Both Bitcoin-NG and Blockene uses member selection in order to select leader or committee respectively. Christopher Natoli et al. [2] provides a summary of different member selection algorithms including their strengths and weaknesses.

References

[1] Ittay Eyal et al. "Bitcoin-NG: A Scalable Blockchain Protocol". In: Santa Clara, CA, USA: Cornell University, 2016. ISBN: 978-1-931971-29-4.

[2] Christopher Natoli et al. “Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure”. In.

[3] Sambhav Satija et al. “Blockene: A High-throughput Blockcain Over Mobile Devices”. In: University of Washington and Microsoft Research India, 2020. ISBN: 978-1-939133-19-9.