Report: Bitcoin-NG: A Scalable Blockchain Protocol

Blockchain has been a huge success in recent past with its features prevailing across online payments , cheap remittance, trust-less asset exchange and machine to machine transfer across countries and currency. The currency without being backed by any major financial institution has earned trust and reliability ($14.9 billion worth of bitcoins were in circulation in January 2017) [1]. Though bitcoin carries stronghold on concepts of decentralization, fairness, safety and security there is one major limitation that is still holding the growth of bitcoin, i.e. scalability [2].

The bitcoin, which is designed to take over currency and decentralization barriers contains a huge potential and it has proved the same in recent past, but it's capable of doing maximum 3.5 transactions per second which is way too less then Visa and Paypal. Bitcoin protocol is designed to add one block every 10 minutes with size of 1 MB , which simply restricts that maximum transactions it can carry is between 1 to 3.5 per second. There have been debates on increasing the size or decreasing the interval but both adds to consequences.Increasing the block size means longer time to transmit, verify, time to win and hence lesser confidence in transaction.On other side, increase in block frequency leads to instability as all nodes will not be able to come to consensus in lesser time[3]. These complications leads to situation where we need to check some out of box solution.

One so possible solution is presented by Bitcoin Next Generation (Bitcoin NG). Its based on same trust model as bitcoin and tries to resolve the scalability problem by breaking blockchain operation into 2 parts i.e key blocks and micro blocks[4].

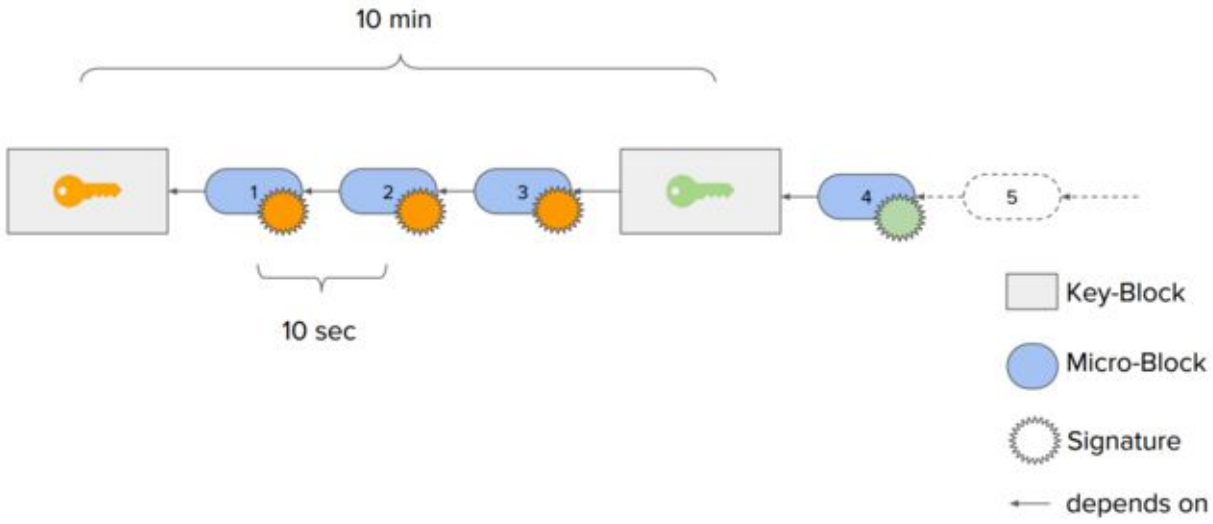
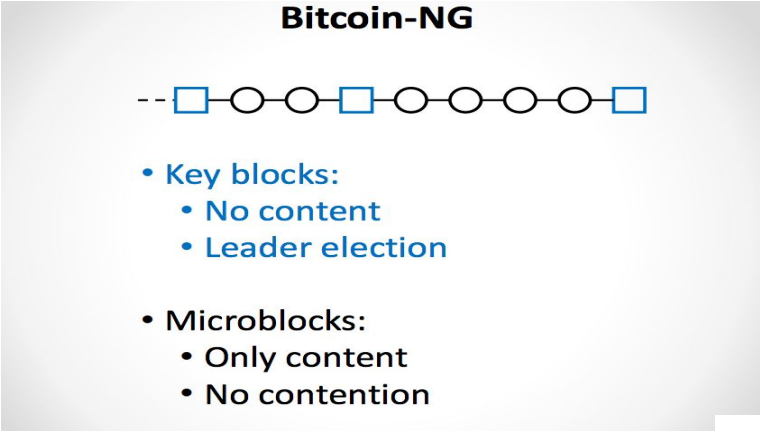


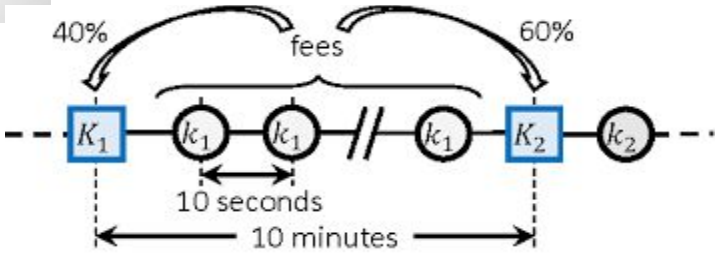
Image from Philipp Jovanovic's 32C3 talk Collective Authorities: Securely Decentralising Trust at Scale[2]

We can relate the Bitcoin approach is like Trucks , a vehicle used to carry load on its back while Bitcoin NG is like a goods train which has a Engine(KeyBlock) allocated just for movement and others coaches(subblocks) carry luggage and but rely on engine for direction.

The new protocol divides times in epochs , each epoch has single leader chosen the same way as bitcoin chooses miner. While the key block has almost same content as bitcoin block ,

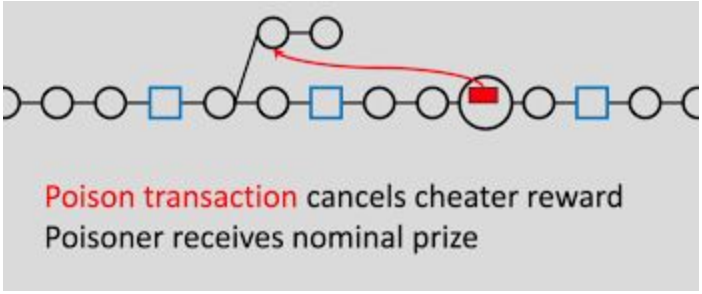


The influence of any leader is valid just for 10 minutes which limit its misuse if an unethical miner is selected as Leader or the machine of leader turns down.



To pay for the efforts for the current miner as well as motivate the subsequent leaders the fee is broken down between present and next leader.

Microblock Fork Prevention

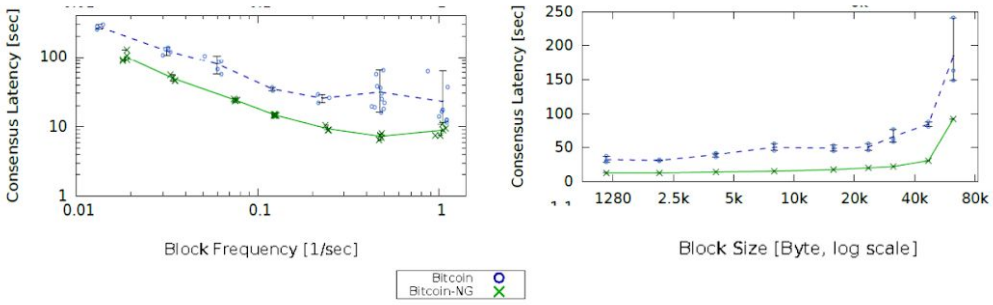


One of major problem with Bitcoin scalability is forks , in Bitcoin NG , the key blocks can be generated by leader and hence pruning can be better managed.

How would it be done without Blockchain - As the paper only discusses about enhancing the existing blockchain protocol , there is not anything that can be done without blockchain as we won't have anything to improve .

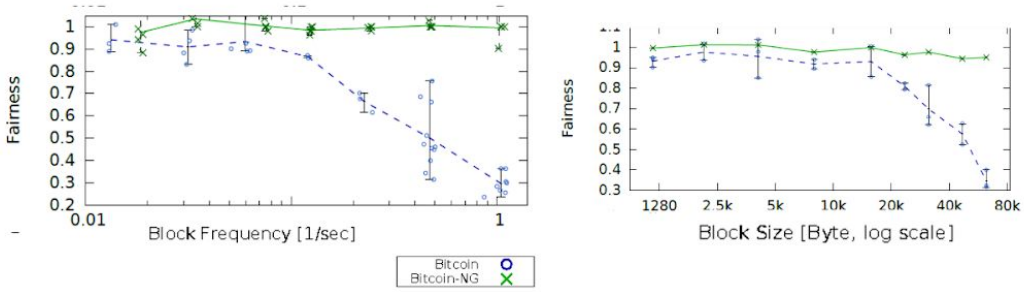
Consensus Delay - Its time system takes to reach common agreement. Higher frequency reduces the consensus latency but NG outperforms the Bitcoin .Also, Increased Block Size yields latency increase for Bitcoin while for NG the increase is miner.

Consensus Delay

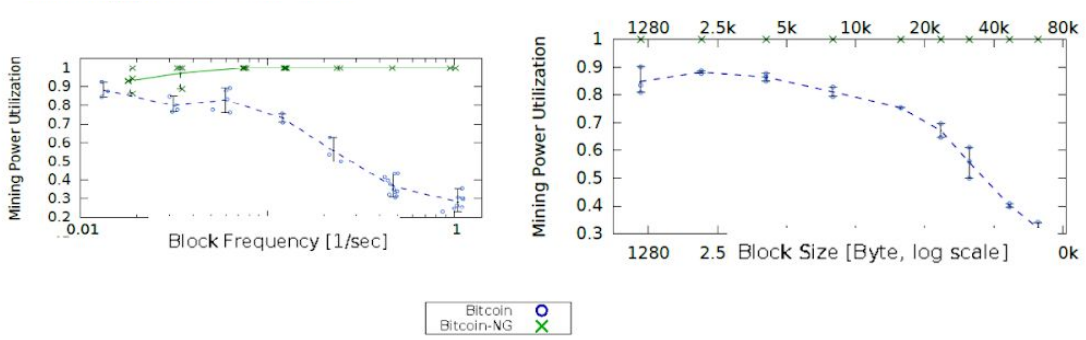


Fairness - Its the ratio responsible to keep the power decentralized. Fairness in Bitcoin NG is not impacted by block size or even frequency as only one miner creates the sub blocks and other miners catch up.

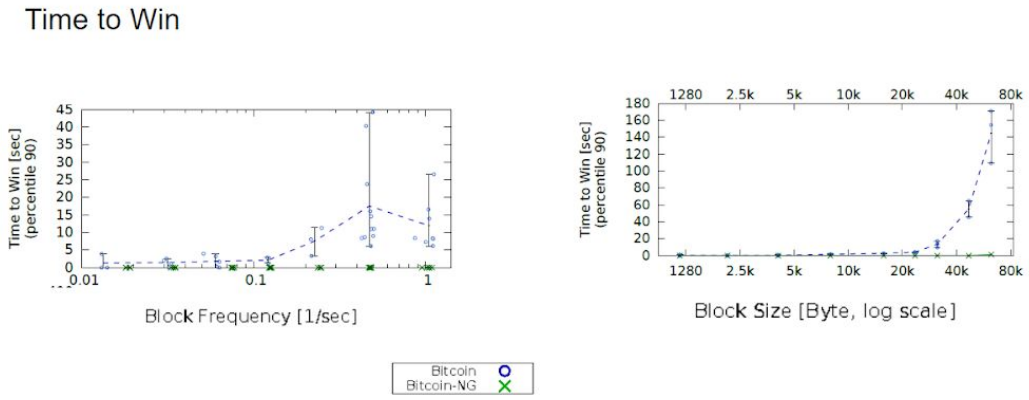
Fairness:



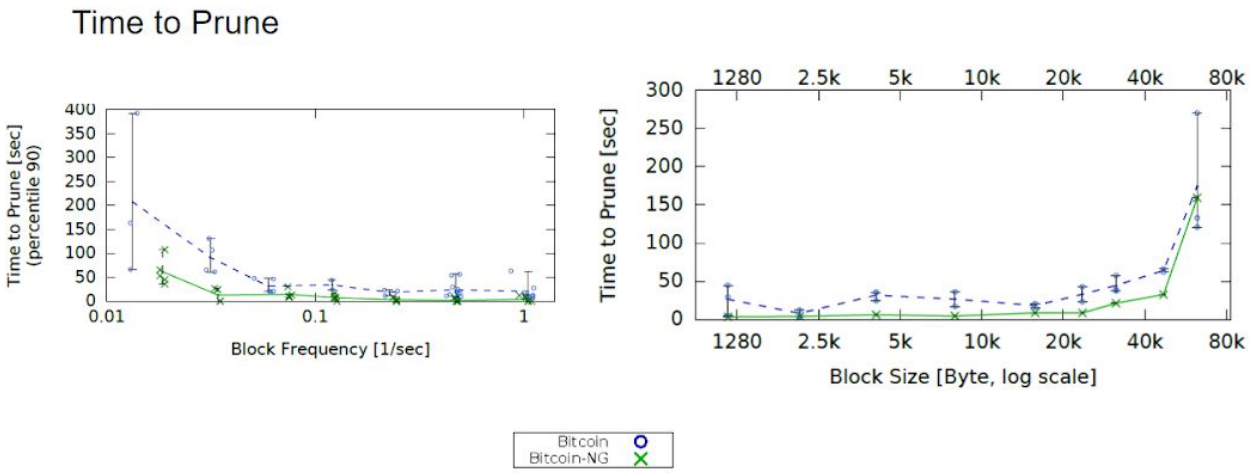
Mining power utilization - It drop quickly for increased frequency, Bitcoin - as by the time a miner get to know about a generated bitcoin , the other miner has already mined other blocks while in NG only the leader generates the main chain blocks.



Time to Win - For Bitcoin, it increases with increase in block frequency as miners struggle to keep up with the leading pack. Also with increase in Block size , as blocks propagates slow and hence it takes more time to decide the leading chain. In NG the forks are likely to be resolved by leading miner.



Time to Prune - For Bitcoin it gets better with increased frequency as more blocks are added per unit time hence making pruning faster while it deteriorates with increased block size as large blocks take time to forge.



Summary

Bitcoin NG proves to be more scalable than Bitcoin on almost many evaluation criteria. The addition of keyblocks adds power to leader that reduces time to win and consensus delay by considerable amount while enhancing mining power utilization and fairness. Time to prune shows little improvement with Bitcoin NG but this area still remains a challenge and need more research in future to come up with a full proof solution to problem of scalability. Bitcoin NG shows it is possible to improve the scalability of the blockchain protocol to a point where consensus latency is only limited only by network diameter and Node's processing power is only bottleneck left in throughput.

References

1) Kindergan, A. (2018). *Is Bitcoin Safe?*. [online] Credit Suisse. Available at: https://www.credit-suisse.com/corporate/en/articles/news-and-expertise/is-bitcoin-safe-201701.html [Accessed 17 Nov. 2018].
2) ARCIERI, T. (2018). *On the dangers of a blockchain monoculture • Tony Arcieri*. [online] Tony Arcieri on Svbtle. Available at: https://tonyarcieri.com/on-the-dangers-of-a-blockchain-monoculture [Accessed 17 Nov. 2018].
3) Wattenhofer, R. (2018). *On Scaling Decentralized Blockchains*. [online] link.springer.com. Available at: https://link.springer.com/chapter/10.1007/978-3-662-53357-4_8 [Accessed 1 Dec. 2018].
4) BANO, S., AL-BASSAM, M. and DANEZIS, G. (2018). *The Road to Scalable Blockchain Designs*. [online] Sheharbano.com. Available at: https://sheharbano.com/assets/publications/usenix_login_2017.pdf [Accessed 17 Nov. 2018].
5) SCHNEIDER, F. B. Bitcoin-NG: A Scalable Blockchain Protocol, included in the Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI ’16) March 16–18, 2016 • Santa Clara, CA, USA.