Scalability Trilemma in PoW Blockchain Networks

Malhar Alpesh Patel

April 2025

1 Introduction

The Proof-of-Work (PoW) consensus algorithm, created by Satoshi Nakamoto in 2008, paved the way for a decentralized secure network where consensus could be achieved between all parties. It introduced the social aspect of incentivizing miners to keep the network running while discouraging malicious behaviors. It has been used successfully in Bitcoin and other cryptocurrencies. However, keeping the network secure and decentralized has come at the cost of scalability. While traditional digital payment systems can handle thousands of transactions every second, Bitcoin manages a mere 7 to 10 transactions per second. This led Vitalik Buterin, the cofounder of Ethereum, to introduce the Scalability Trilemma.

Lemma 1. *Scalability Trilemma.* There is a trade-off between decentralization, security and scalability in blockchain networks - it is only possible to achieve two of them - never all three simultaneously.

This trilemma has not been proven for every blockchain network, and various solutions like sharding, sidechains and state channels have been proposed to overcome it. We show that in an ideal PoW Network based off the original Bitcoin whitepaper though, the scalability trilemma most probably holds true, and this is demonstrated through simulations and theoretical results.

2 Ideal Proof-of-Work Network

An ideal PoW Network can be represented as a graph with the nodes being the miners and the edges being the connections through which blocks propagate. For simplicity, we can convert any such graph into a complete graph with delays built into the newly added edges.

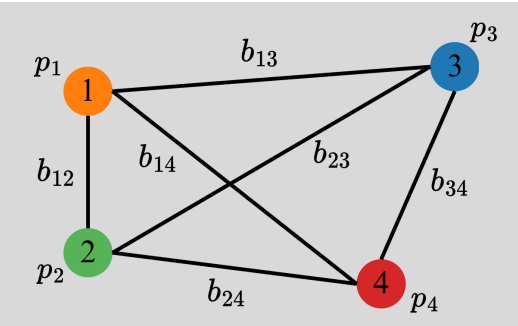

Figure 1: Ideal PoW Network with 4 Miners (Nodes)

where,

- p_i represents hashrate share of node i

- b_{ij} represents bandwidth of edge ij
- t_{avg} is the pre-defined average block mining time for the network
- t_i is the time node i takes to mine its next block
- Probability that node i mines the next block, $P_m(i) = p_i$

With

$$p_i \left(\sum p_i \right) \sim \text{Pareto}(\alpha, x_m = 1)$$

and

$$t_i \sim \text{Exp}\left(\frac{p_i}{t_{\text{avg}}} \right)$$

It takes $\dfrac{M}{b_{ij}}$ time for M transactions to go through edge ij

3 Defining Measures

One of the biggest hurdles in proving the Scalability Trilemma is agreeing on how to measure decentralization, security and scalability. We have looked across the literature available on this and settled on the following measures.

3.1 Decentralization

We use three measures to determine the decentralization of the network - the Gini coefficient, the Nakamoto coefficient, and the Half-Power Bandwidth.

3.1.1 Gini Coefficient

$$\text{Gini} = \frac{1}{2N} \sum_{i=1}^{N} \sum_{j=1}^{N} |p_i - p_j|$$

The Gini Coefficient measures the hashrate share inequality between the miners. It is 1 if the network is completely centralized (one miner owns 100% of the hashrate) and 0 if the hashrate is distributed equally (every miner has an equal hashrate).

3.1.2 Nakamoto Coefficient

$$\text{Naka} = \min \left\{ k \mid \sum_{i=1}^{k} p_{f_i} > 0.5,\ f : [1, N] \to [1, N] \right\}$$

The Nakamoto Coefficient measures the minimum number of miners who when combined exceed 50% of the total hashrate. The higher it is, the more decentralized the network is.

3.1.3 Half-Power Bandwidth

$$b_{0.5} = N \left(\sum_{i=1}^{N} \left(\min \left\{ b_{ik} | \sum_{j=1}^{k} p_{f_j} \ > \ 0.5 \right\} \right)^{-1} \right)^{-1}$$

where $b_{0.5}$ is the Half-Power Bandwidth. It measures the average bandwidth for a block to propagate across more than 50% of the total hashrate. The higher it is, the more decentralized the network is.

3.2 Security

We use three measures to determine the security of the network - the Fork Rate, the Fork Ratio, and the Stale Ratio.

3.2.1 Fork Rate and Ratio

$$F_{\text{rate}} = \frac{\text{number of forks}}{\text{total time}}$$

$$F_{\text{ratio}} = \frac{\text{number of forks}}{\text{length of longest chain}}$$

Temporary forks occur when two or more miners mine a block on top of the same parent block (since they have not yet received the other miners' blocks). A high fork rate and fork ratio indicates poor security as it results in a lower consensus and presents an opportunity for an attacker to take advantage of the longer confirmation times. It also leads to a higher stale ratio as one of the temporary forks will have to be abandoned.

3.2.2 Stale Ratio

$$S_{\text{ratio}} = \frac{\text{number of stale blocks}}{\text{total number of blocks}}$$

A stale block is one that is not part of the longest chain in the long run.

3.3 Scalability

We use one measure to determine the scalability of the network - the TPS (transactions per second).

3.3.1 TPS

$$\text{TPS} = \frac{\text{total number of transactions in longest chain}}{\text{total time}}$$

$$\text{max TPS} \approx \frac{\text{maximum block size}}{t_{\text{avg}}}$$

A higher max TPS (transactions per second) possible in a payment system leads to faster transaction and confirmation times, which increases the overall convenience of using the system.

4 Simulation Results

To improve scalability, we will try to increase the TPS.

4.1 Increase Maximum Block Size

Here,

$$\text{Max TPS} = \frac{\text{Max Size}}{t_{\text{avg}}}$$

and,

$$\text{Half-Power Time} = \frac{\text{Max Size}}{b_{0.5}}$$

Network	Max Size	Max TPS	Half-Power Time	$F_{\text{rate}} \times 10^{-3}$	S_{ratio}	TPS
1	250	2.5	7.436	1.12	0.106	2.462
2	500	5	14.87	1.65	0.170	4.156
3	1000	10	29.74	2.05	0.231	8.307
4	2000	20	59.49	2.66	0.327	13.86
5	4000	40	118.98	2.92	0.425	20.95
6	8000	80	238.0	4.48	0.596	34.65

Table 1: Max Block Size varied from 250 to 8000 with fixed $t_{\text{avg}} = 100$

Increasing the maximum size leads to an increase in TPS with diminishing returns, as it fails to scale up to the maximum TPS possible (compare the Max TPS and TPS columns).

This happens because the increase in block size leads to propagation delays, increasing the Half-Power Time. Once this time approaches t_{avg}, the fork rate increases, leading to most of the blocks being mined becoming stale. These stale blocks do not contribute to the TPS, hence the diminishing returns on increasing block size.

In addition, the increased fork rate and stale ratio measures also negatively affect network security.

The only way to counter the increased fork rate and stale ratio is to increase the average block mining time, t_{avg}, to combat the increased propagation delay time. This, however, brings us back to square one by decreasing the TPS again (since max TPS $\approx \frac{\text{Max Block Size}}{t_{\text{avg}}}$)

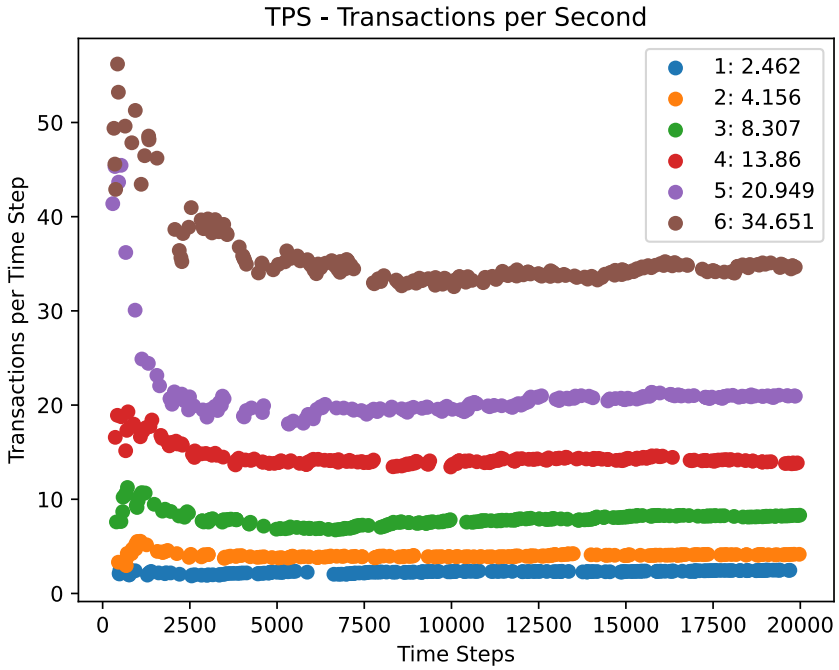

Figure 2: TPS for Increased Maximum Block Size

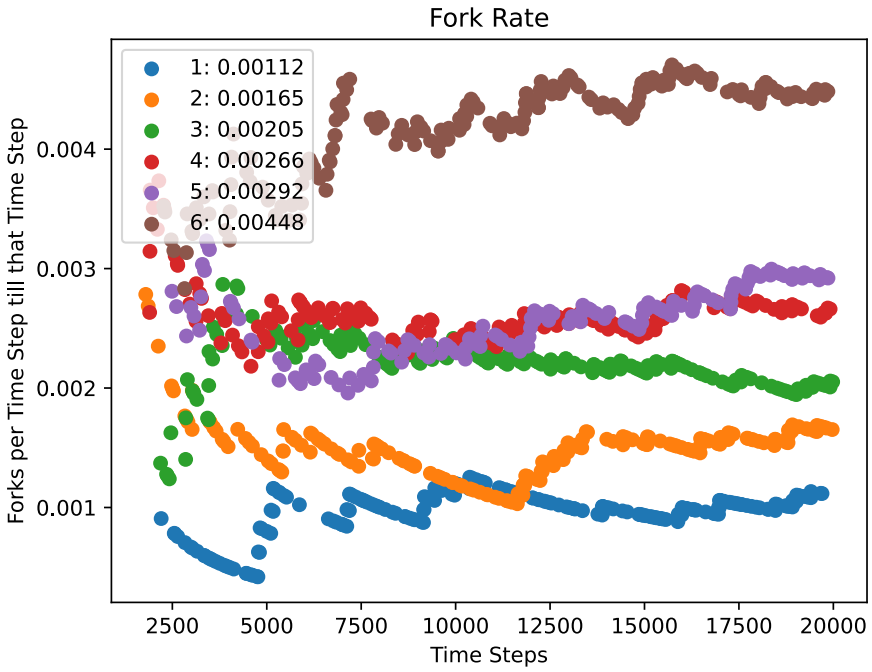

Figure 3: Fork Rate for Increased Maximum Block Size

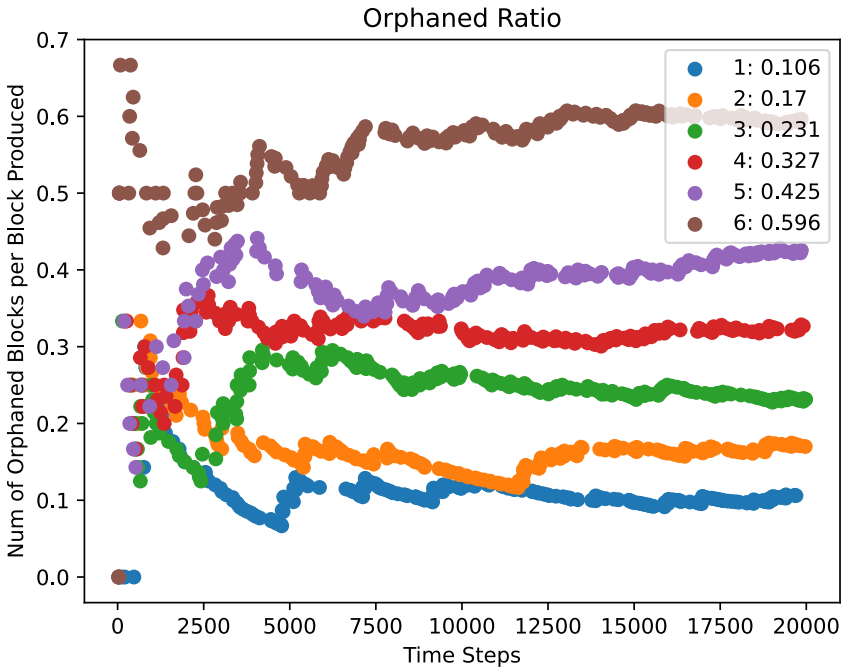

Figure 4: Stale Ratio for Increased Maximum Block Size

5 Theoretical Results

Lemma 2. *Fork Probability.* The probability of n forks occuring after a block has been mined is given by the following formula:

$$\text{Prob}(n \text{ forks}) = \sum_{i \in I} p_i \left(\sum_{A \in C(I_i, n)} \exp\left(-\text{TPS} \sum_{k \in A^C} \frac{p_i}{b_{ik}} \right) \prod_{j \in A} \left(1 - \exp\left(-\text{TPS} \frac{p_i}{b_{ij}} \right) \right) \right)$$

where,

- I is the set of all miners, with $|I| = N$
- $I_i = I - i$, with $|I_i| = N - 1$
- $C(I_i, n)$ denotes the class of all n choices from I_i, with $|C(I_i, n)| = \binom{N-1}{n}$
- A^C denotes the complement of set A

Proof.

$$\text{Prob}(n \text{ forks} \mid i \text{ mines}) = \sum_{A \in C(I_i, n)} \prod_{j \in A} \text{Prob}\left(t_j \leq \frac{M}{b_{ij}} \right) \prod_{k \in A^C} \text{Prob}\left(t_k > \frac{M}{b_{ik}} \right) \tag{1}$$

$$= \sum_{A \in C(I_i, n)} \prod_{j \in A} \left(1 - \exp\left(-\frac{p_i}{t_{\text{avg}}} \frac{M}{b_{ij}} \right) \right) \prod_{k \in A^C} \exp\left(-\frac{p_i}{t_{\text{avg}}} \frac{M}{b_{ik}} \right) \tag{2}$$

$$= \sum_{A \in C(I_i, n)} \prod_{j \in A} \left(1 - \exp\left(-\text{TPS} \frac{p_i}{b_{ij}} \right) \right) \exp\left(-\text{TPS} \sum_{k \in A^C} \frac{p_i}{b_{ik}} \right) \tag{3}$$

$$\text{Prob}(n \text{ forks}) = \sum_{i \in I} \text{Prob}(i \text{ mines}) \text{Prob}(n \text{ forks} \mid i \text{ mines})) \tag{4}$$

$$= \sum_{i \in I} p_i \left(\sum_{A \in C(I_i, n)} \exp\left(-\text{TPS} \sum_{k \in A^C} \frac{p_i}{b_{ik}} \right) \prod_{j \in A} \left(1 - \exp\left(-\text{TPS} \frac{p_i}{b_{ij}} \right) \right) \right) \tag{5}$$

Assuming that every block mined contains the same number of transactions, M, the result above predicts the probability of n forks occurring after a block has been mined. It links the fork rate with TPS. However, calculating this on a computer takes exponential time and is infeasible for any network with more than 17 nodes.

6 Conclusion

We can conclude that based on the framework described in this report for measuring decentralization, security and scalability, the Scalability Trilemma holds true in the ideal Proof-of-Work Blockchain Network. This has been verified through both simulations and theoretical results.

7 Future Work

We plan on expanding this work by experimenting with different measures (like confirmation time as a part of scalability and security). We also plan on exploring the scalability trilemma in other blockchain networks with different consensus mechanisms (like proof-of-stake and proof-of-history) and analyze the cryptocurrencies which claim to have overcome it.

8 Acknowledgements

This work was done under the guidance of Prof. Kalpesh Kapoor and was built upon previous work done by Aastha Gupta. The simulations were run on the 'forty-two' cluster provided by IISER Pune.

9 References

1. *Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto)*
2. *Distributed Ledger Technology: The Science of the Blockchain (Roger Wattenhofer)*
3. *SoK: Measuring Blockchain Decentralization (Ovezik et al.)*
4. *Measuring Decentralization in Emerging Public Blockchains (Jia et al.)*