Poster: 80% of Block Propagation Rate is Enough – Towards Secure and Efficient PoW-based Blockchain Consensus

Daehwa Rayer Lee, Yunhee Jang, Hanbin Jang, and Hyoungshick Kim
Sungkyunkwan University
{dhwa1206,gdb1226,hanbin,hyoung}@skku.edu

CCS CONCEPTS

• **Security and privacy** → Distributed systems security.

ACM Reference Format:
Daehwa Rayer Lee, Yunhee Jang, Hanbin Jang, and Hyoungshick Kim. 2019. Poster: 80% of Block Propagation Rate is Enough – Towards Secure and Efficient PoW-based Blockchain Consensus. In *The 17th Annual Int'l Conference on Mobile Systems, Applications, & Services (MobiSys '19), June 17–21, 2019, Seoul, Korea.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3307334.3328666

1 INTRODUCTION

Recently, Samsung released Galaxy S10 supporting the cryptowallet feature [5]. However, it is still questionable whether cryptocurrency can be popularly used for mobile payments because processing transactions in existing blockchain systems are too slow. For example, public blockchain systems such as Bitcoin [6] (7 transactions per second (TPS)) and Ethereum (15 TPS) are significantly slower than mainstream payment systems such as Visa (2,000 TPS) using a centralized database.

To improve the throughput of blockchain systems, there exist two possible straightforward strategies: (1) Increase block size and (2) Reduce the block interval. Increasing block size improves throughput, but the resulting bigger blocks take longer to propagate in the network. Reducing the block interval can decrease latency, but leads to instability where the system is in disagreement [3]. Therefore, the optimal selection of block size and block interval becomes one of the most challenging issues in designing blockchain systems for a trade-off between security and performance. Here, we focus on minimizing the block interval for blockchain systems using a Proof of Work (PoW) consensus algorithm while maintaining the stability and security of blockchain systems.

In a typical blockchain system, the block interval is set to be greater than or equal to the block propagation time so that a miner is not allowed to generate a new block before all nodes would receive the last block. In this paper, we found that the block propagation rate is critical to achieve a trade-off between security and throughput. Therefore, the block interval should be carefully selected to control the block propagation rate. As a case study, we analyzed the Ethereum network and found that its block interval can be reduced to 1 second without sacrificing security in theory.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
MobiSys '19, June 17–21, 2019, Seoul, Korea
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6661-8/19/06.
https://doi.org/10.1145/3307334.3328666

Releated work. Satoshi [6] proposed a PoW mechanism with the longest chain rule for consensus among Bitcoin nodes. Most popular blockchain systems such as Bitcoin and Ethereum are currently using a PoW consensus algorithm to maintain their blockchain status. In Bitcoin, the block interval of 10 minutes was specifically chosen by Satoshi as a trade-off between security and performance. However, Decker and Wattenhofer [2] demonstrated that the 10 minutes block interval would be overly conservative and could be reduced. For this reason, in Ethereum, 12 seconds was chosen [1] as the block interval based on the findings of real-world Bitcoin network latency (12.6 seconds [2]). Gervais et al. [4] analyzed the security and performance implications of various parameters such as block size and block interval used in PoW consensus algorithms.

2 CONTRIBUTIONS

Given a blockchain system with stable block propagation time, our goal is to find the optimal block interval to maximize throughput of the blockchain system without significantly sacrificing security.

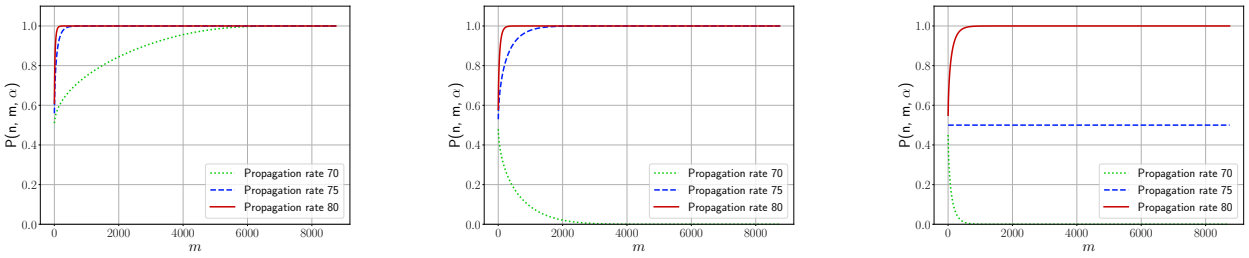
In this paper, we only focused on the demonstration of the feasibility of our analysis framework on the Ethereum network. However, our technique is generic and can be made applicable to other PoW-based blockchain systems such as Bitcoin.

Suppose that a new block b is created by an honest user and then another new block $\bar{b}$ is created by an attacker who tries to intentionally generate a fork. In this situation, an attack becomes successful if a majority of the mining power in the network believes that the attacker's block $\bar{b}$ is the first announced valid block. In other words, we can say that the status of a given blockchain is safe when a majority of the mining power in the network believes that b is the first announced valid block.

We use the notation $P(n, m, \alpha)$ to represent the probability that a given blockchain system is safe where n is the number of total miners in the system; m is the number of nodes receiving new block information during the block interval; and α is the rate of the node believing $\bar{b}$ as the first announced valid block at the worst case, which is the sum of attacker's mining power and the mining power of nodes which did not receive b in the block interval. Without loss of generality, we assume that all miners have the exactly same mining power if all the nodes have the same probability of receiving valid block messages. $P(n, m, \alpha)$ can be calculated as follows:

$$P(n,m,\alpha) \geq \sum_{i=max(\lceil \frac{m+1}{2} \rceil, m-\alpha n)}^{min(m,(1-\alpha)n)} \binom{(1-\alpha)n}{i}\binom{\alpha n}{m-i} / \binom{n}{m} \quad (1)$$

In Equation (1), the equality is obtained only in the case where all nodes which did not receive the block b as the first announced valid block believe that $\bar{b}$ is the first announced valid block. Thus, given n, m, and α, we use Equation (1) to calculate the minimum



(a) Attacker's mining power = 0.19 **(b) Attacker's mining power = 0.22** **(c) Attacker's mining power = 0.25**

Figure 1: Calculation of $P(n, m, \alpha)$ with various environments.

$P(n, m, \alpha)$. Figure 1 demonstrates the minimum $P(n, m, \alpha)$ with various environments.

As shown in Figure 1, it is critical for security to maintain the block propagation rate which is greater than a certain threshold. For example, when $m = 6,000$, the block propagation rate of 70% is sufficient against an attacker with 0.19 mining power. However, if $m \leq 4,000$, the block propagation rate of 70% is not sufficient against the same attacker. Interestingly, if we increase the block propagation rate to 80%, $P(n, m, \alpha)$ becomes close to 1 regardless of m even when attacker's mining power is 0.25. Based on this finding, we recommend the minimum block propagation rate has to be 80%.

In practice, the most effective method is to decrease the block size in order to boost the block propagation rate. However, because this approach can significantly affect TPS of the system, we do not consider it. Another promising technique is to reduce the overlap of block propagation time periods between subsequent blocks.

To demonstrate the feasibility of our analysis framework, we measured the actual block propagation time in the Ethereum network. On April 17th, 2019, we traced 6,360 blocks in total and calculated the block propagation rate every 0.25 seconds. 8,748 nodes were averagely working on the network. Figure 2 plots the mean and standard deviation (which are represented as error bars) of block propagation rates in the Ethereum network.

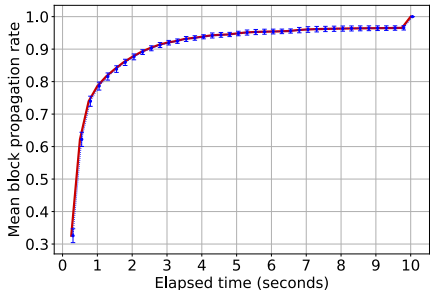


Figure 2: Mean block propagation rate over time in the Ethereum network.

As shown in Figure 2, the mean block propagation rate of Ethereum rapidly increases toward 1 until the elapsed time is less than 1 second and then tends to be smooth and flat—approximately 80% nodes receive the first announced valid block within 1 second on average while the rest receive the block in 9 seconds.

Under such network conditions in Ethereum, we expect that the block interval of Ethereum could be reduced to 1 second while still maintaining the mean block propagation rate of the Ethereum network which is greater than about 80% necessary for security (see Figure 1). Such reduction of the block interval would significantly improve TPS of Ethereum.

3 CONCLUSION

In this paper, we present a framework to analyze the relationship between the number of total miners in a blockchain system, the attacker's mining power, and the block propagation rate in terms of security. We found that the block propagation rate is critical to provide security against an attacker with a certain amount of mining power. Therefore, we need to carefully control the block interval by adjusting the mining difficulty in order to provide a reasonable level of the block propagation rate.

Based on our analysis, in the case of Ethereum, the block interval can be reduced to 1 second without significantly sacrificing security. Thus, TPS of Ethereum would be simply improved by setting the block interval which is much smaller than the current 12 seconds.

As a part of future work, we plan to apply our evaluation framework to other blockchain systems such as Bitcoin using a PoW-based consensus mechanism in order to generalize our findings.

Acknowledgements. This work was supported by the ICT R&D program of IITP (2017-0-00045, Hyper-connected Intelligent Infrastructure Technology Development).

REFERENCES

[1] Vitalik Buterin. 2014. Ethereum Design Rationale. https://github.com/ethereum/wiki/wiki/Design-Rationale Accessed on: 2019-04-13.
[2] Christian Decker and Roger Wattenhofer. 2013. Information propagation in the Bitcoin network. In *Proceedings of the 13th IEEE International Conference on Peer-to-Peer Computing*.
[3] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. 2016. Bitcoin-NG: A Scalable Blockchain Protocol. In *Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation*.
[4] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the Security and Performance of Proof of Work Blockchains. In *Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security*.
[5] Shannon Liao. 2019. The Samsung Galaxy S10 has a cryptocurrency wallet built in. https://www.theverge.com/2019/2/25/18233131/samsung-galaxy-s10-bitcoin-cryptocurrency-wallet-features
[6] Nakamoto Satoshi. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). https://bitcoin.org/bitcoin.pdf Accessed on: 2019-04-13.