Accelerating Block Propagation in PoW Blockchain Networks with Pipelining and Chunking (PiChu)

Kaushik Ayinala
kapnb@mail.umkc.edu
University of Missouri - Kansas City
Kansas City, MO, USA

Baek-Young Choi
choiby@umkc.edu
University of Missouri - Kansas City
Kansas City, MO, USA

Sejun Song
sjsong@umkc.edu
University of Missouri - Kansas City
Kansas City, MO, USA

ABSTRACT

Blockchain is an open, verifiable, and distributed consensus of transactions among different parties, relying on P2P technology for connectivity between nodes. However, the long time of block propagation limits inceptions of another consensus. We propose a novel method that accelerates block propagation in PoW blockchain networks by pipelining message transaction and verifications in parallel over a network with chunks of a block (PiChu). We have conducted extensive evaluations to present the significance of the network pipelining with many parallel chunk connections. Various simulation results exhibit that the proposed method achieves significantly less latency of block propagation than traditional method as the size of a P2P network increases.

KEYWORDS

blockchain networks, scalability, block propagation, chunking, pipelining

1 INTRODUCTION

Blockchain allows a group of nodes to come to an agreement by using consensus. All the nodes in the network follow the consensus to add a block to the chain. The chain acts as ledger for transactions. Proof of Work (PoW) is one of the commonly used consensus algorithms introduced in bitcoin [8]. In PoW consensus, miner has to solve a hash with specific requirements. As a node propagates a winning block over a network, its performance is limited by the underlying P2P layer, which causes the scalability problems in blockchain [4, 5, 7]. By accelerating block propagation, it can minimize the time gap for the inception of another consensus. Therefore, it improves the scalability of the blockchain.

In this work, we propose a Pipelining and Chunking scheme for blockchain networks, named *PiChu* that is to expedite a block propagation by verifying PoW with a block header and forwarding body of the block as small chunks incrementally over the P2P network, instead of a whole block after PoW is completed. After receiving a chunk, a node will verify and forward the chunk. Our experimental results with varied sizes of P2P networks demonstrate significant less latency of block propagation than the traditional method.

2 RELATED WORK

There are a number of studies to improve the scalability of the blockchain network by using multiple chains [9], sharding [7] and faster block propagation [3, 6]. These studies does not use the chunking and pipelining scheme. To the best of our knowledge, this is the first that employs such a scheme for PoW blockchain networks. Furthermore, the proposed scheme can be used along with existing scaling and acceleration techniques in a complementary manner.

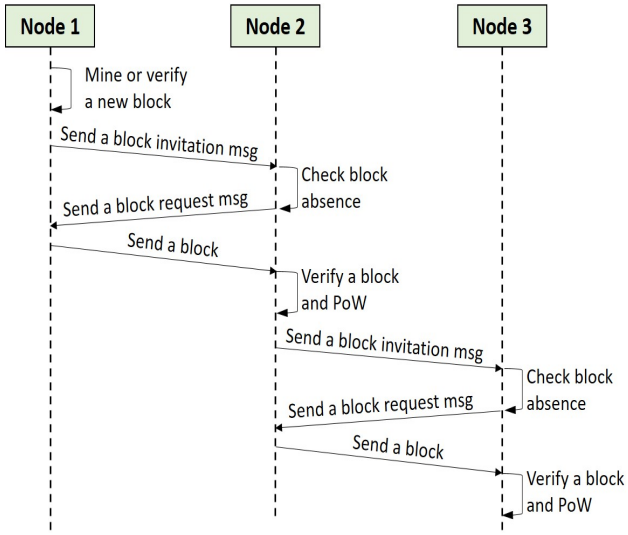

Figure 1: Block propagation sequence in traditional blockchains

3 PICHU: PROPOSED PIPELINING AND CHUNKING SCHEME

In a traditional blockchain networks, when a node mines or receives a block, it sends an invitation to all the neighboring peers, as shown in Figure 1. The node received a block invitation message sends a block request message back to the original node, if it does not have the block. When it receives the complete block, it verifies a block and PoW. After adding the new block, it sends a block invitation message to its neighbor nodes. As presented in Equation (1), it takes the entire block to verify the PoW.

$$Hash(Block) < Target\_Difficulty \quad (1)$$

The proposed PiChu (Pipelining and Chunking) scheme is to expedite the block propagation by verifying PoW with a block header and forwarding as chunks instead of the whole block. PiChu modifies the traditional block structure into a PiChu header that contains fields to validate chunks, identify the position of the block and verify the PoW. A miner signs each chunk and his public key is included in header. As illustrated in Figure 2, when a node mines

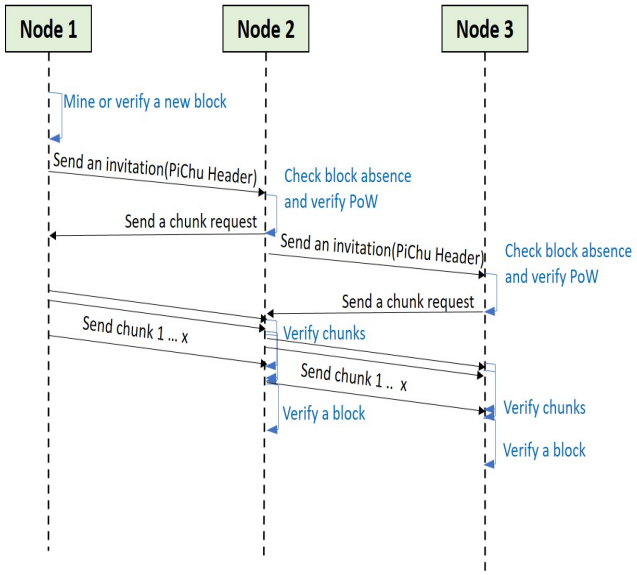

Figure 2: Block propagation in PiChu blockchain

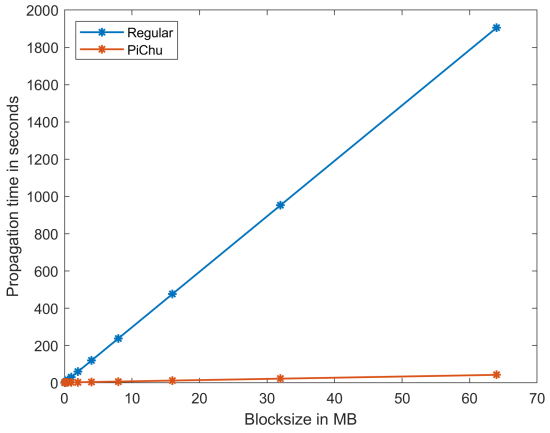

Figure 3: Block propagation time comparison: Regular vs. PiChu (with chunk size of 128 KB, in a 65536 node network)

or receives a block, it sends an invitation to all the connected nodes with the PiChu header. The node received an invitation message sends a chunk request message back to the original node, if it does not have the block and can verify PoW. As shown in Equation (2), it takes only a small header to verify the PoW.

$$Hash(PiChuBlockHeader) < Target\_Difficulty \quad (2)$$

Besides, it sends an invitation message to its neighbor nodes by using the PiChu header. When it receives chunks, it verifies the signature each chunk by using the public key of the miner. Although an additional 64 bytes as a signature is required for each chunk, the overhead is trivial. As long as a whole chunk is verified, it forwards the chunk to its neighbor nodes, which sent a chunk request. Finally, each node verifies a complete block.

4 EXPERIMENT RESULTS

In order to validate the effectiveness of the PiChu scheme in a very large network with varied parameters, we have developed an in-house blockchain simulator. Though there is an existing blockchain simulator called Simblock [2], it is not optimized for evaluations with a large number of nodes. Our simulator is developed in java, and the source code is available in github [1]. We used the average bandwidth of nodes, average latency between nodes, block size, chain length, number of nodes and maximum connections for a node (C_M) as input parameters. For a given number of nodes, the simulator generates a random graph topology based on the number of maximum connections per node. We first assessed how the block propagation times vary depending on the number of nodes and size of the block in general blockchain. We then assess the block propagation times with the varied number of nodes and the size of the block in the blockchain using PiChu propagation technique. Both experiments are conducted under the same constraints. As shown in Figure 3, PiChu achieves less latency in block propagation than the traditional method, and the gain significantly increases with large size of blockchain networks.

5 CONCLUSION

We proposed a pipelining and chucking scheme for a block propagation to accelerate the consensus of blockchain networks. Through various simulations, we have shown that the proposed scheme can greatly reduce the propagation time, thus increase throughput and capacity of a blockchain, making it scalable for a large number of nodes in a blockchain network.

REFERENCES

[1] [n.d.]. PiBhu Blockchain Simulator. http://github.com/dans-lab/BlockchainSimulator.
[2] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo. 2019. SimBlock: A Blockchain Network Simulator. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 325–329. https://doi.org/10.1109/INFCOMW.2019.8845253
[3] Wei Bi, Huawei Yang, and Maolin Zheng. 2018. An Accelerated Method for Message Propagation in Blockchain Networks. *CoRR* abs/1809.00455 (2018). arXiv:1809.00455 http://arxiv.org/abs/1809.00455
[4] Joan Donet, Cristina Pérez-Solà, and Jordi Herrera-Joancomartí. 2014. The Bitcoin P2P Network, Vol. 8438. https://doi.org/10.1007/978-3-662-44774-1_7
[5] 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 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 3–16. https://doi.org/10.1145/2976749.2978341
[6] Jia Kan, Lingyi Zou, Bella Liu, and Xin Huang. 2018. Boost Blockchain Broadcast Propagation with Tree Routing. *CoRR* abs/1810.12795 (2018). arXiv:1810.12795 http://arxiv.org/abs/1810.12795
[7] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. 2016. A Secure Sharding Protocol For Open Blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 17–30. https://doi.org/10.1145/2976749.2978389
[8] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (03 2009). https://bitcoin.org/bitcoin.pdf
[9] Jiaping Wang and Hao Wang. 2019. Monoxide: Scale out Blockchains with Asynchronous Consensus Zones. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. USENIX Association, Boston, MA, 95–112. https://www.usenix.org/conference/nsdi19/presentation/wang-jiaping