Proximity Neighbor Selection in Blockchain Networks

Yusuke Aoki, and Kazuyuki Shudo
Tokyo Institute of Technology
2-12-1 Ookayama, Meguro, Tokyo, Japan

***Abstract*—Blockchains have attracted a great deal of attention as a technology for the distributed management of register information at multiple nodes without a centralized system. However, they possess the drawbacks of low transaction throughput and long approval time. These problems can be addressed by shortening the block generation interval; however, shortening this interval alone has the effect of increasing the frequency of forks. In this study, we aim to shorten the block generation interval without increasing the fork generation rate by improving the network topology of the nodes and shortening the propagation time. We propose a neighbor node selection method forming a network topology with a short block propagation time. A blockchain simulator is used to demonstrate the effect of the proposed neighbor node selection method on the propagation delay of the network. This result indicates that the proposed method improves block propagation time.**

***Index Terms*—blockchain, neighbor selection, peer-to-peer**

I. Introduction

Blockchain is a distributed ledger technology that appeared as the core technology of the cryptocurrency Bitcoin [1], which is developed by the name of Satoshi Nakamoto. In recent years, many cryptocurrencies using blockchain have been ledger developed and operated, and blockchains have attracted increasing attention. Blockchains can manage information securely and protect it from tampering, even if multiple malicious nodes are present. Additionally, no central management is required, and a blockchain system can operate independently. These features have proven to be very useful, and their application is being studied not only in cryptocurrency but in a wide range of fields.

Although blockchains have many advantages, they also have several drawbacks. The primary problems involve the low throughput of transactions and the approval time for a transaction. These obstacles can be overcome by shortening the block generation interval. However, if the block generation interval alone is shortened, the block propagation time will not be sufficiently shorter than the block generation interval; consequently, the frequency of forks will increase, leading to increased security risk [2].

In this study, we construct a network topology with a short block propagation time as a policy for overcoming the aforementioned challenges. Because a blockchain network is a peer-to-peer network without a central management system, the network topology is determined by each node's selection of neighbor nodes. Therefore, in this paper, we propose a neighbor node selection algorithm for forming a network topology with a short block propagation time. In the proposed algorithm, each node evaluates other nodes using a score based on the speed of block delivery, and preferentially selects a node with a good score to be a neighbor node. An improved block propagation time can be achieved if each node dynamically changes neighbor nodes based on information that can be obtained during blockchain operation.

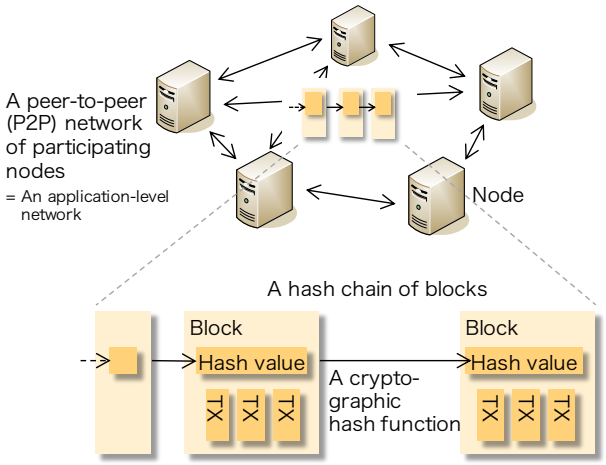

Fig. 1. Blockchain overview.

Using a simulator, we demonstrated that the proposed neighbor node selection algorithm improves block propagation time.

The remainder of this paper is structured as follows. Section II provides background information on blockchains, while Section III proposes a neighbor node selection algorithm to improve transaction throughput. Section IV describes experiments performed using a simulator to confirm the proposed method. Section V presents conclusions and ideas for future work.

II. Blockchain

Blockchain is a distributed ledger technology regarded as part of Bitcoin, proposed by Satoshi Nakamoto. The nodes of a blockchain constitute a peer-to-peer network. Because blockchains have no central management, a consensus algorithm has been devised to ensure a consistent ledger without contradiction between nodes. Most blockchain consensus algorithms are Byzantine fault-tolerance [3] and have the useful feature that even if a malicious node intentionally propagates false information, the blockchain can form a correct consensus.

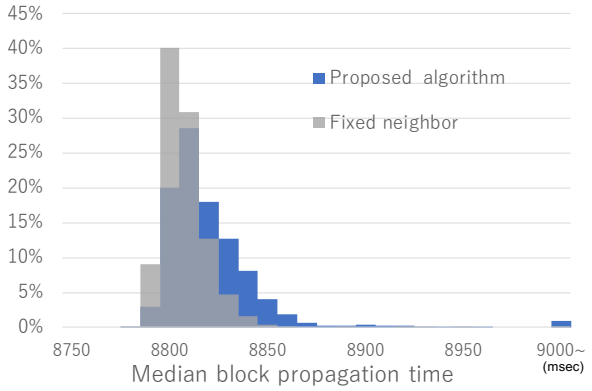

Fig. 12. Median of the propagation time for uniform network enviroment.

proposed algorithm and the fixed-neighbor algorithm.

It can be seen that the block propagation times are distributed in a very narrow range for a uniform network, and there is no improvement in propagation efficiency with the proposed algorithm. In this experiment, the median propagation time of the top 100 nodes with the highest block generation performance was slightly lower than the median overall propagation time. Nodes with high block generation performance are considered to be concentrated at the center of the network. If nodes with a favorable network environment participate in a blockchain network, efficient block propagation may occur because nodes with high block delivery speed tend to be located near the center of network, where nodes with high block generation performance are concentrated.

V. Conclusion

The major drawbacks of blockchains include low transaction throughput and the long approval times. These problems can be addressed by shortening the block generation interval; however, if the block generation interval alone is shortened, the occurrence of forks rises and the security risk increases. Thus, it is necessary to shorten the block propagation time in order to shorten the block generation interval while suppressing the occurrence of forks. In this study, we developed a neighbor node selection algorithm to form a network with a short block propagation time. In a blockchain network, each node rates other nodes according to the speed of block delivery, and preferentially selects a node with a good score to be a neighbor node. With our proposed algorithm, a network with hight block propagation efficiency can be formed using only information that each node can obtain locally. Using a simulator, we confirmed that the proposed neighbor node selection algorithm improves block propagation time.

Future work should examine additional block propagation protocols used in existing blockchains. Protocols other than the traditional ones used in this paper have been proposed. A famous example is the compact block relay [17]. In a traditional block propagation protocol, if the transaction in a received block is already present in the transaction pool, this implies that the same transaction has been received twice In the compact block relay protocol, when receiving block, the bandwidth used in suppressed by receiving only transactions that are not included in the transaction pool. When the proposed algorithm is used in a blockchain employing compact relays, the influence on bandwidth of neighbor node selection is reduced, and the propagation delay and block generation performance are expected to improve.

Future work should also investigate changes to the security of the network resulting from the proposed neighbor node selection algorithm. Because the proposed algorithm alters the network topology, we must investigate what influence it has on resistance to fragmentation and other attributes by analyzing the graph of the network.

Acknowledgment

This work was supported by SECOM Science and Technology Foundation.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[2] Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in Bitcoin. In *Proc. FC'15*, 2015.
[3] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
[4] Bitcoin Core: Bitcoin. https://bitcoincore.org, (accessed May. 30, 2019).
[5] Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee. Discovering Bitcoins public topology and influential nodes. 2015.
[6] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102, 2018.
[7] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. On scaling decentralized blockchains. In *Proc. Financial Cryptography and Data Security 2016 (FC16)*, pages 106–125. Springer, 2016.
[8] Visa acceptance for retailers. https://usa.visa.com/run-your-business/small-business-tools/retail.html, (accessed May. 30, 2019).
[9] PayPal, Inc — PayPal reports first quarter 2019 results. https://investor.paypal-corp.com/news-releases/news-release-details/paypal-reports-first-quarter-2019-results, (accessed May. 30, 2019).
[10] Christian Decker and Roger Wattenhofer. Information propagation in the Bitcoin network. In *Proc. IEEE P2P 2013*, pages 1–10, 2013.
[11] Takehiro Miyao, Hiroya Nagao, and Kazuyuki Shudo. A method for designing proximity-aware routing algorithms for structured overlays. In *Proc. IEEE ISCC'13*, 2013.
[12] K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker, and I. Stoica. The impact of DHT routing geometry on resilience and proximity. In *Proc. ACM SIGCOMM 2003*, August 2003.
[13] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on Bitcoin's peer-to-peer network. In *24th USENIX Security Symposium*, pages 129–144, 2015.
[14] Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, and Kazuyuki Shudo. SimBlock: A blockchain network simulator. In *Proc. 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019)*, 2019.
[15] Ryohei Banno and Kazuyuki Shudo. Simulating a blockchain network with SimBlock. In *Proc. 2019 IEEE Int'l Conf. on Blockchain and Cryptocurrency (IEEE ICBC 2019)*, pages 3–4, 2019.
[16] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of Proof of Work blockchains. In *Proc. ACM CCS 2016*, pages 3–16, 2016.
[17] bip-0152.mediawiki. https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki, (accessed May. 21, 2019).