On-chain Scaling of Blockchain

Akihiro Fujihara
Department of Information and Communication Systems Engineering, Chiba Institute of Technology
2-17-1 Tsudanuma, Narashino, Chiba 275-0016, JAPAN
akihiro.fujihara@p.chibakoudai.jp

Since Bitcoin appeared in 2008, blockchain technology has been gaining considerable public attention. The words "block chain" were born from a dialogue between the Bitcoin inventor, Satoshi Nakamoto, and a cryptographer, Hal Finney, on the cryptography mailing list [1]. Blockchain is a chain of block-structured databases where each block is connected in a time-series order by a cryptographic hash function, and works as a timestamp server. Actually, blockchain is not a new idea, as the citing of Massias *et al.*'s paper published in 1999 [2] in Nakamoto's white paper suggests. However, it has become an iconic image for related technologies.

All transactions in Bitcoin, including the issuance and exchange of electronic cash, are disclosed on the blockchain. Therefore, nodes participating in the peer-to-peer (P2P) network can verify which address (not user) holds how many bitcoins by tracking transaction records. However, since users can keep as many bitcoins addresses as they want, it is difficult for others to know how much Bitcoin one owns in total. Therefore, a minimum level of user's privacy is considered. Transaction processing is completed when a transaction is saved to the blockchain through a high-load computational process called Proof of Work (PoW) [3]. Any node can become an *authority* that connects a block with transactions to the blockchain by presenting evidence to other nodes that it is able to execute the PoW correctly and quickly. Therefore, the system is designed so that no particular node can remain as an unjustified authority. In addition, PoW also makes transaction records on the blockchain tamper-resistant.

Personal transaction information has been kept private due to privacy concerns. However, Bitcoin has made all transaction records public with privacy in mind (although anonymity is not guaranteed). This makes it possible for an unspecified number of nodes to reach a (extended) consensus about transaction records on the blockchain on the basis of the longest-chain rule. Because this consensus algorithm was essentially a new idea, compared with known ones in distributed systems, it is called *Nakamoto Consensus* (仲基合意).

The essential value of Bitcoin is *Micropayment*, which is possible by reducing the transaction fee to an extremely low level, such as less than one cent or one yen. Micropayment has the potential to create a new decentralized economy, as it enables charging for various operations performed on the Internet. For example, Wikipedia, which is always struggling to collect donations, may be able to collect server maintenance fees from very small donations from many article readers by introducing micropayment. However, the current blockchain technology is practically incapable of supporting micropayment because the transaction processing capacity is restricted by the block transfer speed between nodes and the limit of block size, which is known as the *Bitcoin scalability problem*.

Several technologies have been studied to solve this problem. Off-chain scaling technologies, such as Lightning Network [4], are currently attracting attention. Off-chain technologies leave less transaction records in the blockchain. Bitcoin has been used as a payment means of conducting illegal transactions in darknet markets, and there have been many reports on the managers and users of these markets being arrested [5]–[7]. These arrests are attributable to Bitcoin's disclosure of all transactions with tamper resistance, which are available as legal evidence. If off-chain scaling technologies become widespread, transactions that cannot be audited by our societies and governments can be easily created. Then, off-chain services might become hotbeds of illegal transactions in darknet markets and money laundering by criminal organizations. Thus, when we consider the use of blockchain technology on the basis of law and ethics, it is ultimately necessary to solve the scalability problem on-chain.

There are naive methods to solve the problem on-chain: increasing the block size and shortening the block-generation-time interval. Both are possible by increasing the communication speed between nodes, but it gets difficult for nodes with slow communication speed to join the network. The former method is being experimented on Bitcoin Scaling Test Network (STN) [8]. While the maximum block size of Bitcoin Core is 1 MB, STN has eliminated the block size limit, and has achieved an average transaction processing capacity of 1,875 transactions per second in the latest 144 blocks [8] (Accessed on 25 May 2021). The latter method is also being considered by bloXroute [9]. This project proposes to improve scalability by introducing a backbone network to propagate large blocks in a shorter time.

Existing blockchains, such as Bitcoin, are based on the premise that only one blockchain can be globally integrated and managed. As a result, blocks are transferred and shared among nodes all over the world, which slows down transaction processing speed. As a way of speeding up transactions, we have proposed a mechanism for allocating domains to geographically close nodes, similar to the country code top-level domain in the Domain Name System, and managing blockchains in each domain [10]. Through this mechanism, it is possible to distinguish between the inside and outside of a domain by the communication speed with the central node,

which is the entrance to the P2P network. In addition, our mechanism allows domain-specific geographic information to be handled by connecting secure Internet-of-Things devices to some of the nodes. However, the domain partition entailed by our mechanism reduces the number of nodes participating in each domain, which degrades the decentralization and tamper resistance of the blokchain.

To solve this problem, we proposed a cross-referencing method for periodically exchanging the state of the latest fixed block in the blockchain with hysteresis signatures among all the domains via the upper network layer (Layer-0) [11]. We also designed a communication protocol to autonomously execute our cross-referecing method among domains. Furthermore, we evaluated the effectiveness of our method from the theoretical viewpoints of decentralization, scalabitily, and tamper resistance.

Since the definition of decentralization is often ambiguous, we will define it as the ability of every participating node to affect the entire system by creating blocks. With our method, in-domain decentralization is equivalent to that of usual public blockchains, such as Bitcoin. Out-domain decentralization is preserved by hysteresis signatures, which affect some of the blocks in other domains.

We roughly estimated the average transaction (TX) processing capacity in the proposed system, *i.e.*,

$$T \simeq 3,000[\text{TX/sec.}] \times \frac{SN}{I}, \tag{1}$$

where S [MB] is the average block size, N is the number of domains, and I [sec.] is the average block-generation-time interval. In the case of Bitcoin Core, $S = 1$ MB, $N = 1$ domain, and $I = 600$ seconds. Then, $T \simeq 5$ transactions per second. Regarding scalability in transaction processing capacity, the performance of the entire system can be improved because transactions and blocks are distributed only inside the domain. For example, if the block size is increased to $S = 12$ MB, the number of domains to $N = 200$, and the average block-generation-time interval to $I = 120$ seconds, the transaction processing capacity becomes $T \simeq 60,000$ transactions per second, which can reach an equal or better level compared with that of VISA credit card system where $T \simeq 56,000$ transactions per second in peak performance.

For tamper-resistance, each domain has evidence of the hysteresis signatures of the other domains in the blockchain. Therefore, to tamper with a block in a domain, one must also tamper with the blocks containing the relevant hysteresis signatures in all domains. If all relevant blocks are not tampered with, then tamper correction is also possible by checking the hysteresis signature mismatch. We defined a tamper-resistance-improvement ratio, *i.e.*,

$$R = \frac{\sum_d \text{Sum\_of\_Top\_X}(h_{d1}, \cdots, h_{dN_d})}{\text{Sum\_of\_Top\_X}(h_1, \cdots, h_N)}, \tag{2}$$

where h_* is a hash rate of node, Sum_of_Top_X is the function to sum up the top X hash rates of nodes, d is the domain index, N is the total number of core nodes, N_d is the total number of core nodes in the d-th domain, and $\sum_d N_d = N$. To estimate typical R, we conducted Monte Carlo simulations in which the hash rate is randomly assigned in accordance with a Pareto distribution, *i.e.*,

$$f(h_*) = \frac{\alpha}{h_*^{1+\alpha}} \quad (h_* \geq 1), \tag{3}$$

where α is the scale parameter. We assume that $X = 10$, $N = 10,000$, and the number of core nodes in each domain is uniform, *i.e.*, 10, 100, and 1000 nodes when the number of domains is 1000, 100, and 10, respectively. As a result, we confirmed that tamper resistance improves more as the total number of domains becomes larger. We concluded that it is possible to achieve a more scalable and tamper-resistance public blockchain balanced with decentralization using our cross-referencing method.

In addition, we are implementing a central node using Python to evaluate the theoretical performance experimentally [12]. We are conducting our experiment using the reference implementation, and confirmed that the cross-referencing method succeeds across five domains.

REFERENCES

[1] A record of when the words "block chain" were firstly used: https://satoshi.nakamotoinstitute.org/emails/cryptography/6/#selection-37.36-37.47 (Accessed on 25 May 2021)

[2] H. Massias, X. S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirement," 20th Symposium on Information Theory in Benelux (1999)

[3] A. Back, "Hashcash - A Denial of Service Counter-Measure" (2002) http://www.hashcash.org/papers/hashcash.pdf (Accessed on 25 May 2021)

[4] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (2016) https://lightning.network/lightning-network-paper.pdf (Accessed on 25 May 2021)

[5] FBI, "Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website " (2013) https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (Accessed on 25 May 2021)

[6] The US Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down" (2017) https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (Accessed on 25 May 2021)

[7] The US Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin" (2019) https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

[8] Bitcoin Scaling Test Network https://bitcoinscaling.io/ (Accessed on 25 May 2021)

[9] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "bloXroute: A Scalable Trustless Blockchain Distribution Network," White paper (2018) https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf (Accessed on 25 May 2021)

[10] A. Fujihara, "PoWaP: Proof of Work at Proximity for a crowdsensing system for collaborative traffic information gathering," Internet of Things, 100046, Elsevier (2019)

[11] T. Yanagihara and A. Fujihara, "Considering Cross-Referencing Method for Scalable Public Blockchain," EIDWT 2021, Lecture Notes on Data Engineering and Communications Technologies, vol. 65, pp. 220-231, Springer (2021)

[12] T. Yanagihara and A. Fujihara, "Experimental implementation of the cross-referencing method for scalable public blockchain", https://github.com/cit-fujihalab/crossref_BC, (Accessed on 25 May 2021).