Performance Evaluation Experiments of Bitcoin SV Scaling Test Network

Akihiro Fujihara and Takaaki Yanagihara

Abstract The Bitcoin SV Scaling Test Network (STN) is an experimental network for solving the scalability problem of Bitcoin with on-chain technology. A large amount of transactions are always transmitted on P2P networks, and experiments are conducted to generate huge blocks. In this study, by constructing the STN node, the occupancy rate of transaction processing and the branch probability of the blockchain are estimated. As a result, the estimated occupancy rate was about 1.04 and the estimated branch probability was 8.5%. In addition, the transaction processing performance was experimentally evaluated by transferring transactions including the OP_RETURN script at a high frequency of once per minute for a period of one week. As a result, the probability of the transaction being processed into BC was 98%. It was also confirmed that the latency distribution taken for transactions to be processed in tended to follow a power-law distribution at the tail. From the above, the consideration by the queueing theory with priority seems to be effective even in STN.

1 Introduction

The origin of blockchain is a theoretical study on distributed timestamp services for electronic documents by Haber and Stornetta in the early 1990s [1, 2, 3]. At that time, the Internet was insufficiently developed, and it was difficult to use the proposed system in a real environment. However, the real environment was prepared by the time that Bitcoin [4] appeared in 2008, and the operation of the peer-to-peer

Akihiro Fujihara
Chiba Institute of Technology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016, JAPAN, e-mail: akihiro.fujihara@p.chibakoudai.jp

Takaaki Yanagihara
Chiba Institute of Technology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016, JAPAN, e-mail: s1522313qq@s.chibakoudai.jp

eletronic cash system started on January 3, 2009. Since then, the system has never stopped working. As a result of this achievement by Bitcoin, the word "Blockchain" (Hereinafter abbreviated as BC) was born and it has attracted attention though it is essentially the same technology as the distributed time stamp services. Therefore, the new idea created by Bitcoin was not BC, but Nakamoto Consensus (仲基合意), where an unspecified number of nodes participating in the network form a consensus on BC. Although research on consensus algorithms had been conducted before the advent of Bitcoin, Nakamoto Consensus was innovative in that it proposed a method to form consensus among unspecified number of nodes on the Internet scale by combining multiple mechanisms such as Proof of Work (PoW)[5, 6], longest-chain rule, and incentive mechanism.

The innovative use value of Bitcoin is in micropayments of less than one yen or cent that can be realized by making transaction fees extremely low. Micropayment makes it possible to collect near zero (the level at which people don't care about paying) charges from a large number of users when using various services on the Internet. Micropayments therefore have the potential to create new decentralized economic mechanisms that have never existed before. However, the current Bitcoin Core (BTC) [7] is not used for ordinary payments as an electronic money system, but has become a store-of-value system for speculative purposes. Behind this, there is a technical issue that make BTC practically difficult to perform many micropayments.

The block size limit of BTC is 1 MB, and blocks larger than this are rejected by miners. The average block generation time interval for BTC is controlled to ten minutes by a difficulty adjustment algorithm. Therefore, the system can only approve transactions that can be recorded in a block of 1 MB at maximum every ten minutes on average. This means that transaction processing capacity is about 7 Transactions Per Second (TPS) at maximum, which is much slower than 56,000 TPS of VISA credit cards. To speed up the transaction processing capacity of a BC system, one might think it becomes better to simply increase the upper limit of block size or shorten the average block generation time interval. However, the larger the block size, the more time it takes to transfer and share the block to all nodes on the P2P network. Therefore, another block is easily generated before the previously generated block is distributed to the whole P2P network, and the probability that the BC is split increases. When the BC is split, the hash rate of nodes that drives block generation is fragmented and its security is degrated. The same problem occurs even if the average block generation time is shorter than 10 minutes. For these reasons, there are technical difficulties in improving the transaction processing capacity, which is called blockchain scalability problem.

Various research proposals have been made to solve the scalability problem [8] and we are also engaged in it with some previous works [9, 10, 11, 12, 13]. Among them, a technique like Lightning network [14], in which a large amount of transactions are executed outside BC, and only the final result is written in BC at once, is attracting attention to reduce the amount of transactions to approve. This called off-chain scaling technique because it avoids the scalability problem by utilizing a system outside BC. Off-chain technology looks good, but individual transaction processing does not remain in BC.

Bitcoin has a history of being used as a means to conduct illegal transactions on darknet markets. In recent years, however, many cases have been reported in which managers and users of these markets have been arrested [15, 16, 17]. These arrests stem from the fact that bitcoin exposes all transactions in a tamper-proof manner, making them available as legal evidence. From this point of view, as off-chain technology spreads, the number of transactions that cannot be tracked and audited by the government increases, making it difficult to control illegal transactions in the darknet market and becoming a hotbed for money laundering. Considering the balance between law and ethics, it is required to solve the scalability problem by the On-chain technology which processes all transactions on BC ultimately.

In order to solve the scalability problem with on-chain, it is necessary to shorten the average block generation time or increase the block size while controlling BC well so that it does not branch. BloXroute[18] is a proposal to improve block propagation speed by connecting a network layer which can propagate larger blocks in a shorter time to P2P network named Blockchain Distribution Network.

The effort to increase the block size is being piloted at Bitcoin SV (BSV) [19] Scaling Test Network (STN) [20]. As mentioned above, the block size limit of BTC is 1 MB, while the block size limit of BSV is eliminated. As of February 9, 2021, this led to an average transaction processing rate of 1,059 transactions per second (TPS) per 24 hours, with the largest block size ever mined reported at 2.9 GB.

This paper reports the results of data analysis and performance evaluation experiments on transaction processing in an environment where the upper limit of block size is eliminated by constructing STN nodes. The contribution of this research is shown below.

- Using the queueing theory, we investigate the time variation of the transaction processing utilization. As the result, it was proven that the estimated working rate exceeded 1 in most time zones.
- Using the function of bitcoin-cli, we estimate the bifurcation probability of BC. The results show that the bifurcation probability is calculated to be about 2% for BTC, but increases to about 8.5% for BSV STN. From this fact, it was also able to estimate by the calculation that the time for transferring the block to the whole node of the P2P network is about 53 seconds.
- We measured the time it takes for transactions containing the OP _ RETURN script to be incorporated into BC when they are transferred at a high frequency of once a minute. As a result, the probability that transactions are incorporated into BC is 98%, and the time distribution tends to follow the power distribution. We also confirmed the tendency to follow a power exponent of 3/2, which is consistent with the theory of priority queueing.

2 Related Works

2.1 Calculation of BC split probability

It is known that the block generation time of bitcoin follows an exponential distribution.

$$F(t) = P(T \leq t) = \int_0^t \lambda e^{-\lambda t'} dt' = 1 - e^{-\lambda t}. \tag{1}$$

where the parameter $\lambda$is the inverse of the average block creation time. For bitcoin, the average block creation time is $1/\lambda = 10$ minutes $= 600$ seconds.

In addition, the time it takes for a block to spread to 90% of the nodes in the P2P network of BTC is measured as $t = \tau_{fork} \fallingdotseq 12$ seconds before Compact Block Relay is applied. Before a block is spread over the whole network, BC branches when another block is generated. Therefore, the probability of the bifurcation of the Bitcoin BC can be calculated as follows.

$$F(\tau_{fork}) = P(T \leq \tau_{fork}) = 1 - e^{-\lambda \tau_{fork}} \fallingdotseq \lambda \tau_{fork} = 12/600 = 0.02. \tag{2}$$

It is shown that the bifurcation probability of BTC is about 2%.

2.2 Theory of Priority Queuing

It is known from the results of theoretical analysis that when the utilization rate is $0 < \rho \leq 1$, the waiting time of low priority customers follows a power distribution with a power exponent of $3/2$, and its base has a cutoff of the exponential distribution[21].

$$P(\tau) = \frac{A}{\tau^{3/2}} \exp(-\tau/\tau_0), \tag{3}$$

$$\tau_0 = \frac{1}{\mu(1-\sqrt{\rho})^2}, \tag{4}$$

$$\rho = \lambda/\mu. \tag{5}$$

where A is the normalized constant of the probability distribution, λ is the average arrival rate of customers, and μ is the average service rate. It has also been reported that the same power distribution is followed when the utilization rate takes the supercritical state $\rho > 1$. The difference from the case of $0 < \rho \leq 1$is that at a rate of $1 - 1/\rho$, customers will be unable to wait for an infinite amount of time, that is, forever.

Previous research[22] has shown that the time it takes for transactions in bitcoin to be imported into BC can be explained by a preferential queueing theory that relies

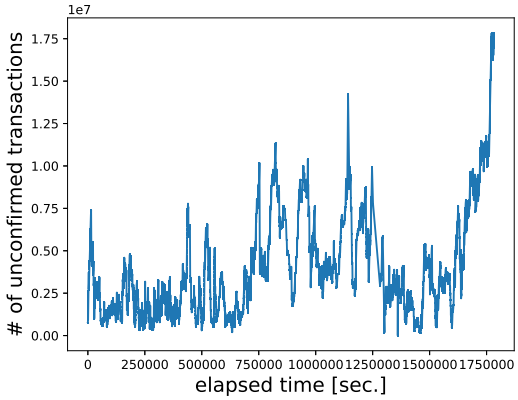

Fig. 1 Trend of Unconfirmed Transactions in STN.

on transaction fees. From this fact, it is expected that the time distribution for the transaction to be taken into BC in BSV STN has the same property.

3 Bitcoin SV Scaling Test Network

BSV started STN as a third test net except RegTest and Testnet to solve the scalability problem of bitcoin by the On-chain technology. In testnet, the block size tends to be small because the number of transactions is small, but in STN, a large number of transactions are sent periodically to make a huge block. Figure 1 shows the time evolution of the number of unconfirmed transactions in the STN.

The data from which this figure is derived are collected and used from whatsonchain[23]. Figure 1 shows that there are regularly more than 1 million transactions in the Transaction pool. It is also found that the number of transactions sometimes reaches more than 10 million. BSV supports the use of OP_RETURN scripts, but most transactions are simply transfers between addresses.

The network of STN is open to the public, and anyone can construct a node and participate in P2P network. However, as system requirements for node construction, performance of 8–16 cores for CPU, 64 GB (+64 GB Swap) for memory, over 3 TB for hard disk, and over 1 Gbit for both up and down Internet connection are required. The total size of BC was 2.4 TB at that time in February 9, 2021. Since it is about 22 GB in Testnet of BSV and 284 GB in Mainnet, it is proven that the capacity of BC is very large in comparison. And, the block height of BC of STN became 15,216 as of February 9, 2021, and it is small, which is because BC has been reorganized several times in the past. Information on the github of the BSV records that BC was reorganized in April and November 2020.

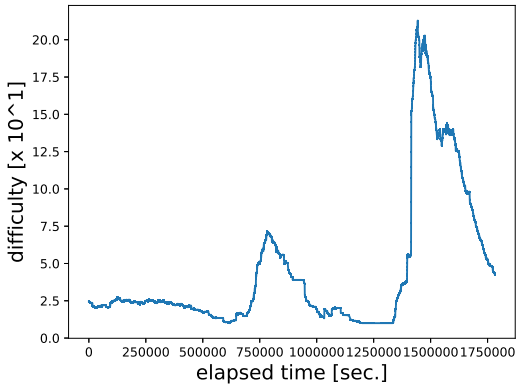

Fig. 2 Block mining difficulty over time.

And, block mining by CPU becomes possible in STN, as it is proven from the system requirement. The time course of block mining difficulty is shown in Fig. 2. The degree of difficulty varies from one to several tens, making mining easy.

It is recommended that STNs be configured with a maximum block size of 10 GB. It is also recommended that Bitcoin scripts be limited to 2GB of memory. Figures 3 show the results of examining the size distribution of blocks mined so far. The block size distribution of STN seems to follow an exponential distribution. The largest block size ever mined was 2.9 GB. On the other hand, the figure below in Figs. 3 shows the block size distribution in Mainnet, which interestingly seems to follow a power distribution rather than an exponential distribution. It also seems to follow the Pareto-Zipf law (= the power-law distribution of the exponent 2) from the tendency of power exponent. STN coins have no market value, but Mainnet has a market value. Though the reason of such difference in the distribution is not well understood, it seems to be influenced by some economic principle when coins with market value are available.

The BSV recommends recording the miner ID on the blocks mined to assess the reputation of the miner. Figures 4 and 5 show the results of calculating the ranking of block mining frequency with reference to this miner ID. Both STN and Mainnet seem to follow a power-law distribution.

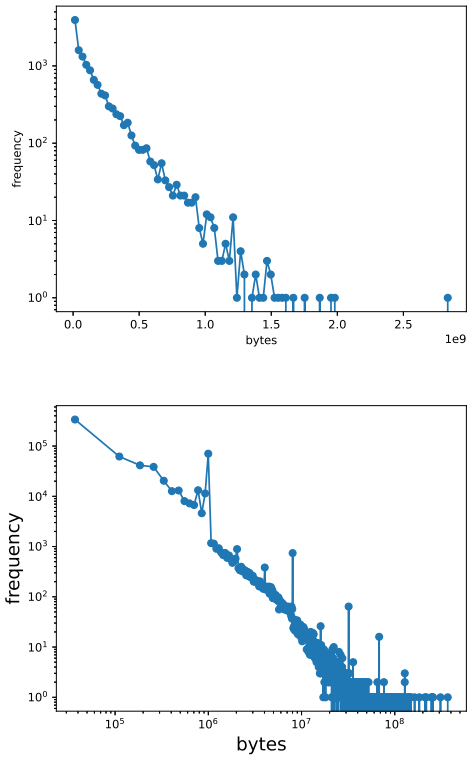

Fig. 3 Block Size Distribution in Bitcoin SV (Above is STN, below is Mainnet).

4 Performance Evaluation Experiments

4.1 Experiment 1: Estimating the Occupancy Rate of Approving Transactions in STN

From the time variation of the number of unconfirmed transactions in Fig. 1, the operating rate of STN was estimated. Figure 6 shows the results of calculating the time variation of the estimated STN utilization rate $\tilde{\rho}$ based on queuing theory. It can be seen that the estimated occupancy rate exceeds 1 in most time periods. This result suggests that there are transactions which are not taken into BC. Using data from November 4, 2020 to February 9, 2021, the estimated occupancy rate was calculated as $\tilde{\rho} \fallingdotseq 1.04$. From these results, it is considered that there is a probability of $1 - 1/\tilde{\rho} \fallingdotseq 0.0387$ that transactions are not included in BC.

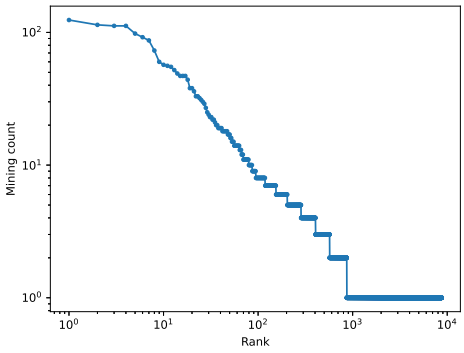

Fig. 4 Block mining frequency ranking calculated with reference to miner ID (STN)

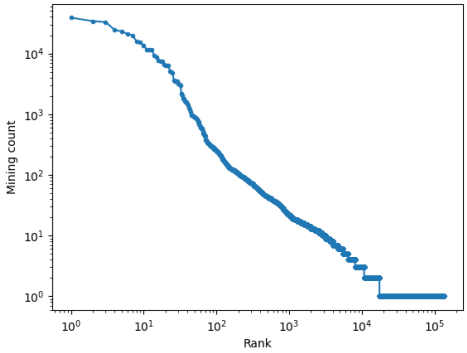

Fig. 5 Block Mining Frequency Ranking Calculated Based on Miner ID (Mainnet)

4.2 Experiment 2: Estimating BC Split Probability

If you build an STN node and connect it to a P2P network, you will see that when you think a large block has been created, a large branch of BC will occur and it will go into Safe mode and you will not be able to transfer money using the bitcoin-cli command. Once a large bifurcation occurs, it can take nearly half a day to resolve. We conducted an experiment to estimate the branching probability from the time when the branching occurred by obtaining the errors value of bitcoin-cli getinfo.

During the period from November 4, 2020 to January 13, 2021, the errors value was collected once every 10 seconds (594,880 times in total). We also counted the number of warnings that BC splits. As the result, following two kinds of warnings were issued.

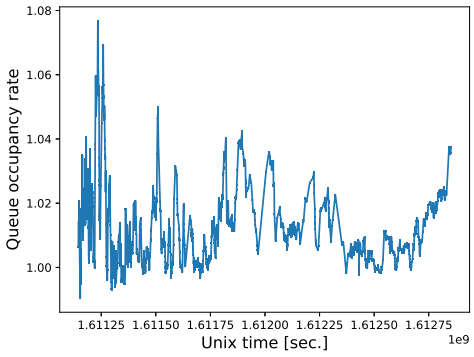

Fig. 6 Time variation of the estimated occupancy rate in STN $\tilde{\rho}$.

- Warning: The network does not appear to fully agree! We received headers of a large fork. Still waiting for block data for more details. (The frequency of occurrence was 32,724 times, accounting for approximately 5.5% in total.)
- Warning: The network does not appear to fully agree! Some miners appear to be experiencing issues. A large valid fork has been detected. (Occurred 17,782 times, accounting for about 3% in total.)

From these results, we can estimate the bifurcation probability to be about $(5.5+3=)8.5\%$. This is about four times larger than the BC-split probability in BTC. By the way, when the split probability of BSV Mainnet was evaluated by the same method, it became 0%. And, when $F(t) = 0.085$ and $\lambda = 1/600$ are substituted in the expression (1), $t = \tau_{fork} \fallingdotseq 53$ seconds, so that the average block transfer time in STN can be estimated to be about 53 seconds.

4.3 Experiment 3: Testing Transaction Processing Performance

In this paper, we experimentally evaluate how long it takes for transactions to be incorporated into BC in the situation that there are always many transactions in the transaction pool.a The experimental period was set for 1 week from January 7 to 14, 2021, and the position information of the civil aircraft which flew around Tsudanuma where Chiba Institute of Technology is located was collected from the collection node of ADS-B data of Flightradar 24 [24] at the frequency of 1 minute always except for the case in which the transaction transmission by the branch is not possible during the period, and the transaction including the data was transmitted as OP_RETURN script. The size per transaction should be less than 63 KB. The transaction fee was fixed at 0.001 BSV. BSV charges more than 1 satoshi/byte. The size of transaction data is large because many commercial aircrafts fly in the daytime,

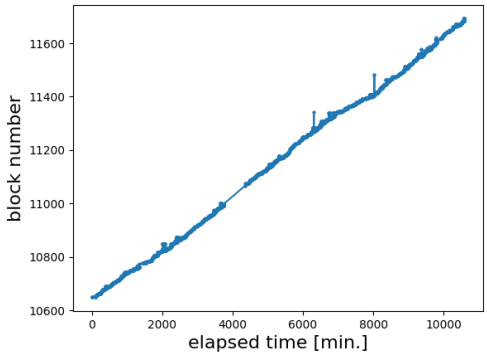

Fig. 7 Correspondence between the elapsed time and the block number where the transaction was captured.

but transactions are not transmitted when there is no data to write, because there is almost no flight at night. Additional details about the results are available on our Github website [1].

Figure 7 shows the correspondence between the elapsed time of the experiment period and the block number in which the transaction was captured. You can see that transactions are regularly captured in blocks over time. On the other hand, it can be confirmed that there are some transactions which are seldom taken into BC.

A total of 6,828 transactions were sent during the experimental period, 104 of which were not incorporated into BC. From this, the probability that the transaction does not get into BC can be calculated as $(104/6828 fallingdotseq)0.02$. This result is almost the same as the result calculated in Fig. 4.1 clause, which estimates that there is a probability of $1-1/\tilde{\rho} \fallingdotseq 0.0387$ that transactions are not approved.

A histogram of the time taken from transaction transmission to incorporation into BC is shown in Fig. 8. Since the block generation time distribution follows the exponential distribution, the time taken into BC follows the exponential distribution in the short term of about half a day, but it deviates from the exponential distribution in the long term of about one week. In fact, as shown in Fig. 8, a linear trend appears in the double-logarithmic plot, which confirms that the trend follows the power distribution. The power index is estimated from the slope of the double-logarithm plot and is close to 3/2. These results are consistent with the theoretical analysis of priority queueing. From this fact, it is anticipated that the transaction with low commission becomes low priority, and that it takes time to be taken into BC.

Figure 9 shows the relationship between the ratio of transaction fees to transaction size and the latency time until a transaction is approved. A low fee rate indicates that it is taking a long time for transactions to be incorporated into BC. Therefore, it is considered that the consideration by the queueing theory with priority is effective even in STN.

[1] `https://github.com/cit-fujihalab/stn_experiments`

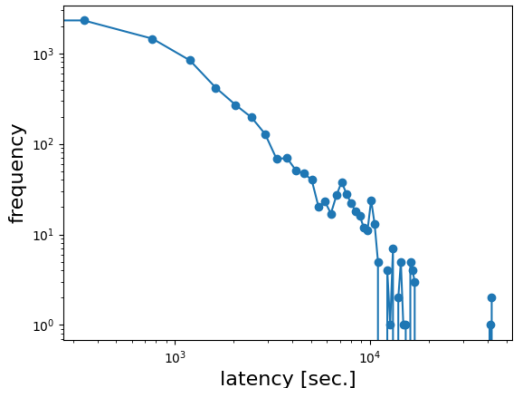

Fig. 8 Histogram of latency time of transaction to be taken into BC.

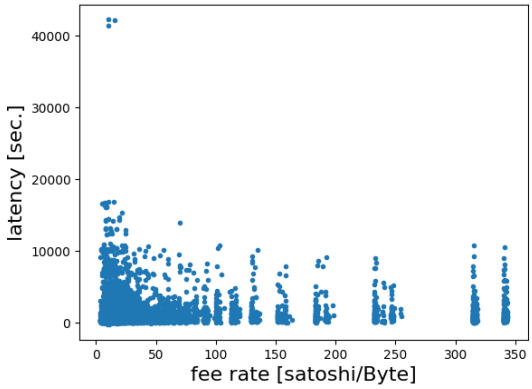

Fig. 9 Relationship between the transaction fee as a percentage of transaction size and the time it takes for the transaction to arrive in BC.

5 Conclusion

In this study, a Bitcoin STN node was constructed, and data analysis and performance evaluation experiment on transaction processing in the environment in which the block size upper limit was removed were carried out. As a result of examining the time variation of the working rate of transaction processing, it was proven that the estimated working rate exceeded 1 in most time zones. Using bitcoin-cli, we also estimated the branching probability of BC, and found that it is about 8.5% for STN, which is more than 4 times the probability of BTC. The average block transfer time of the P2P network was also estimated to be about 53 seconds. The transaction processing performance was experimentally evaluated by transferring transactions containing OP_RETURN scripts at a high frequency of once a minute for a period

of one week. As a result, it was found that the probability of transactions being incorporated into BC was 98%, and its time distribution tended to follow the power distribution in the long term. We also confirmed the tendency to follow a power exponent of 3/2, which is consistent with the theory of priority queueing. From this fact, it can be said that the consideration by the queueing theory with priority is effective even in STN.

For future work, it is necessary to confirm the processing performance when a larger number of transactions are continuously transmitted over a long period of time.

Acknowledgements This work was partially supported by the Japan Society for the Promotion of Science (JSPS) through KAKENHI (Grants-in-Aid for Scientific Research) Grant Number 20K11797.

References

1. S. Haber and W. S. Stornetta, "How To Time-Stamp a Digital Document," J. Cryptology, 3, 99-111 (1991)
2. D. Bayer, S. Haber, and W. S. Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping," Sequences II: Methods in Communication, Security, and Computer Sicence, pp. 329-334 (1993).
3. S. Haber and W. S. Stornetta, "Secure Names for Bit-Strings," CCS'97: Proceedings of the 4th ACM conference on Computer and communications security, pp. 28-35 (1997).
4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (White paper), 2008 https://bitcoin.org/bitcoin.pdf https://www.bitcoinsv.io/bitcoin.pdf
5. C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," Advances in Cryptology (CRYPTO'92), Lecture Notes in Computer Science, vol. 740, Springer (1993).
6. M. Jakobsson and A. Juels, "Proofs of Work and Bread Pudding Protocols (Extended Abstract)," In: Preneel B. (eds) Secure Information Networks, The International Federation for Information Processing, vol 23, Springer (1999).
7. Bitcoin Core https://github.com/bitcoin/bitcoin
8. Q. Zhou, *et al.*, "Solutions to Scalability of Blockchain: A Survey" IEEE Access, Vol. 8, pp.16440-16455, IEEE, 2020.
9. A. Fujihara, "Proposing a System for Collaborative Traffic Information Gathering and Sharing Incentivized by Blockchain Technology," The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018), pp.170-182 (2018) https://link.springer.com/chapter/10.1007/978-3-319-98557-2_16
10. A. Fujihara, "PoWaP: Proof of Work at Proximity for a crowdsensing system for collaborative traffic information gathering," Internet of Things, 100046, Elsevier (2019). https://www.sciencedirect.com/science/article/pii/S254266051830177X
11. A. Fujihara, "Proposing a Blockchain-Based Open Data Platform and Its Decentralized Oracle," Advances in Intelligent Networking and Collaborative Systems (INCoS2019), Advances in Intelligent Systems and Computing, Vol. 1035, pp. 190–201, Springer (2020). https://link.springer.com/chapter/10.1007/978-3-030-29035-1_19
12. T. Yanagihara and A. Fujihara, "Considering Cross-Referencing Method for Scalable Public Blockchain," Advances in Internet, Data and Web Technologies, Lecture Notes on Data Engineering and Communications Technologies, Vol. 65, pp. 220-231, Springer (2021). https://link.springer.com/chapter/10.1007/978-3-030-70639-5_21

13. T. Yanagihara and A. Fujihara, "Cross-Referencing Method for Scalable Public Blockchain," Internet of Things, Vol. 15, 100419 (2021). https://www.sciencedirect.com/science/article/pii/S2542660521000639
14. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (2016) https://lightning.network/lightning-network-paper.pdf
15. 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
16. 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
17. 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
18. U. Klarman, *et al.*, "bloXroute: A Scalable Trustless Blockchain Distribution Network" (White paper), 2018. https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf
19. Bitcoin SV (Satoshi Vision) https://github.com/bitcoin-sv/bitcoin-sv
20. Bitcoin Scaling Test Network https://bitcoinscaling.io/
21. J. G. Oliveira and A.-L. Barabási, "Darwin and Einstein correspondence patterns," Nature 437, 1251, 2005.
22. S. Kasahara and J. Kawahara, "Effect of Bitcoin fee on transaction-confirmation process," Journal of Industrial and Management Optimization, 15 (1): 365-386, 2019.
23. WhatsOnChain.com, BSV Explorer - STN, https://stn.whatsonchain.com/
24. Flight Tracker — Flightradar24 — Track Planes in Real-time, https://www.flightradar24.com/