Proposal of Stable Method of Block Generation Time Considering the Amount of Mining Power in Bitcoin

Daishiro IKOMA*, and Kenya SATO**

(Received February 2, 2021)

In recent years, virtual currencies are in circulation around the world. Bitcoin is a representative of virtual currencies, and the technology that supports the implementation of Bitcoin is blockchain. The Bitcoin blockchain has a mechanism to generate blocks once every 10 minutes, but in reality, the block generation time is greatly changed due to changes in mining power. Therefore, there is concern that the number of transactions and the transaction completion time will not be stable. In this research, we propose a method to adjust the difficulty of mining by changing the mining power and aim to stabilize the block generation time. As a result, the greater the effect of changes in mining power on the overall mining power, the more effective it was. Even in an actual blockchain network, we think that it is effective when the mining power changes significantly.

Key words: bitcoin, blockchain, SimBlock

1. Introduction

In recent years, virtual currencies[1] have been circulated around the world and are attracting attention as decentralized currencies using P2P technology, which has no center anywhere. Bitcoin is a representative of virtual currencies. The technology that supports the implementation of Bitcoin is blockchain. The blockchain works as shown in the Fig. 1. The conventional management system is called a centralized system, and all of the user's transaction data is managed by a server, which is a third-party organization. The existence of a third-party organization has disadvantages such as high cost, unclear transaction data, and easy falsification.

However, the blockchain management system is also called a distributed transaction ledger and has a structure in which users manage each other without going through an administrator. Therefore, the advantages are that the value of information is kept reliable, that it is difficult to falsify, and that the cost of the administrator can be reduced[2]. There are various technologies implemented in the blockchain, but in the Bitcoin blockchain, a consensus building algorithm called Proof-of-Work is used. Proof-of-Work realizes the structure shown in Fig. 2. Each block has a hash value of the previous block to maintain consistency with the previous block. Also, due to the existence of an answer that a miner named Nonce will find in about 10 minutes, the found miner keeps the motivation to get a reward in addition to block generation. It is expected to be applied in various fields due to the difficulty of tampering and decentralization due to the mechanism that miners consume power to find nonces

*Computer and Information Science, Graduate School of Science and Engineering, Doshisha University, Kyoto, Japan.
Email:daishiro.ikoma@nislab.doshisha.ac.jp
**Computer and Information Science, Graduate School of Science and Engineering, Doshisha University, Kyoto, Japan.
Email:ksato@mail.doshisha.ac.jp

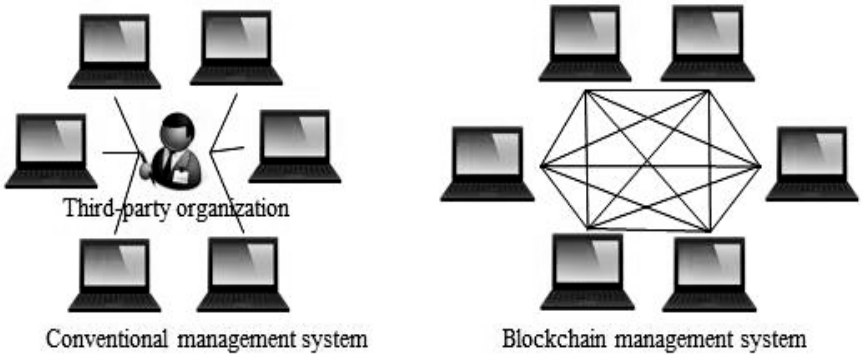

Fig. 1. Comparison of conventional management system and blockchain management system.

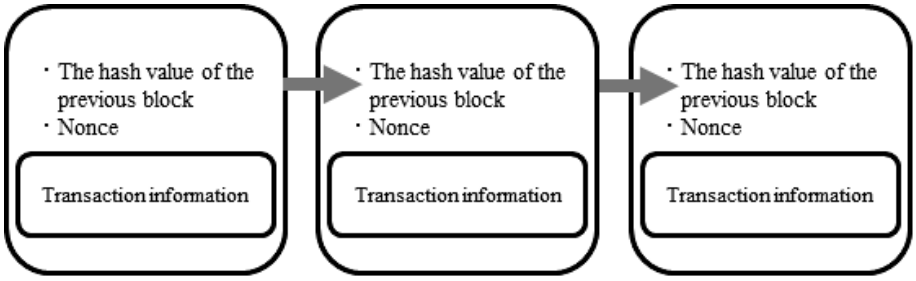

Fig. 2. Blockchain data structure.

and obtain rewards and create new blocks by calculating. Also, the expected value of the nonce discovery time changes depending on the mining power, but the difficulty level of mining is adjusted once every two weeks so that the block generation time will be about 10 minutes even if the mining power changes. As an adjustment method, the difficulty level is adjusted from the average of the block generation time of the last two weeks.

However, the block generation time is not sufficiently stable with this adjustment alone. The result of the mining difficulty adjustment is published[3], for example, the average block generation time for the last two weeks on June 17, 2020 is 8 minutes 42 seconds for him, which greatly increases the difficulty. It is a situation that must be raised. In particular, when the mining power changes suddenly, the block generation time changes significantly, and there is concern that the transaction completion time and the number of transactions will not be stable.

As for the transaction completion time in Bitcoin, the transaction is completed if the blocks are connected up to 6 blocks after the transaction data is written in the block. This is to prevent the transaction data from being destroyed by the branching of the block. This completion time is about 60 minutes[4], but the transaction completion time also changes as the block generation time changes. In addition, since the amount of transactions that can be described in one block is fixed, if the block generation time is delayed, the number of transactions will also decrease, and there is a risk that transactions will be delayed.

Therefore, the purpose of this research is to stabilize the block generation time when the mining power changes suddenly in the Bitcoin blockchain, and to stabilize the transaction completion time and the number

of transactions.

Currently, as a countermeasure against the current situation where the block generation time fluctuates due to changes in mining power, the mining difficulty level is adjusted once every two weeks. However, with the current Bitcoin, the block generation time often changes, and sufficient measures have not been taken, so this study will improve it.

2. Related Research

Blockchain platforms such as Bitcoin, which have a consensus building algorithm called Proof-of-Work, use a difficulty adjustment algorithm to keep the block generation interval constant, and adjust the difficulty of mining. Difficulty is the probability that a miner will get a mining reward when he spends a certain amount of computational resources, and the probability that a block will be generated. However, in the current Bitcoin, even if the mining power changes significantly and a lot of computational resources are consumed, the difficulty level does not change, so the block generation time is not stable.

Against this background, in Hashimoto's paper[5], We thought that the block generation time could be stabilized by adopting the Bitcoin Cash algorithm for Bitcoin. Bitcoin blockchain adjusts the difficulty of mining once every two weeks, while Bitcoin Cash adjusts the difficulty of mining once every 10 minutes. As a result, it was shown that it is possible to keep the block generation interval constant even when the change in mining power is large.

However, Bitcoin Cash has a background that this algorithm was adopted because the number of minors was small and the hash rate was not stable, and since Bitcoin has a large number of minors, the difficulty level is adjusted every 10 minutes. It is considered that the calculation cost is high and there is a lot of waste. In addition, since We am not paying attention to the mining power that causes the block generation time to change, it can be said that the difficulty level of mining is adjusted later.

3. Proposed Method

3.1 *Overview*

Bitcoin blockchain currently adjusts the difficulty of mining by referring to the past block generation time once every two weeks, but we think that it is not enough. Therefore, in addition to the conventional method, we use a proposed method that uses mining power as a judgment material for adjusting the difficulty of mining.

Specifically, the proposed method compares the mining power at a certain point with the current mining power, and if the mining power is increasing, it increases the difficulty of mining so that the block generation time becomes slower. Also, if the mining power is decreasing, it reduces the difficulty of mining so that the block generation time becomes faster. After that, the same thing is repeated based on the mining power after adjusting the difficulty level. In this way, measures are taken so that the block generation time is not affected by changes in mining power as much as possible. In addition, the criteria for adjusting the difficulty level of mining vary depending on the original mining power.

3.2 *Operation procedure*

(1) Obtain the mining power as the original value.
(2) Obtain the mining power as the current value.
(3) If the current value increases or decreases by x% or more of the original value, the mining difficulty level is adjusted. (x is determined by the original mining power)
(4) Repeat steps (2) and (3) until the difficulty level is adjusted.

4. Implementation

4.1 *Overview*

There are various types of blockchain network platforms such as "Hyperledger Fabric" and "Hyperledger Iroha", but in this research, we use the

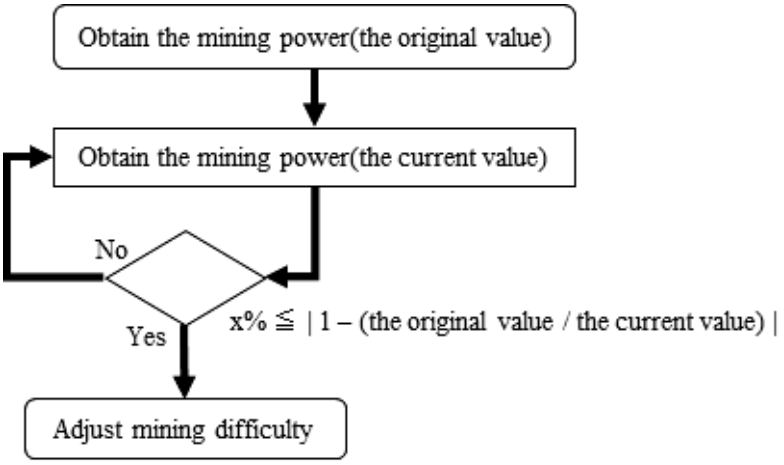

Fig. 3. Operation procedure of the proposed method.

public blockchain simulator "SimBlock[6)]". SimBlock was announced at Tokyo Institute of Technology, released as open source software, and distributed free of charge. SimBlock can simulate a blockchain network on his PC to verify its performance and safety. Furthermore, because it is a public blockchain, it reproduces the Bitcoin blockchain network, and since it is possible to set the number of nodes and mining power, it is suitable for research and actually solves the problems of blockchain. Research is underway to do so[7)].

In this research, we assume a Bitcoin blockchain network, so we will implement and evaluate it using the SimBlock simulator.

4.2 *Blockchain network settings*

In this research, the parameters are set so that they are as close to the Bitcoin blockchain network as possible. It was set. The details of the parameters are shown below.

- Number of nodes: 1000, 5000, 10000 (units)
- Mining power of each node: 100 (MH/sec)
- Block height: 2000
- Expected block generation time: 600 (sec)
- Block size: 0.5 (MB)

5. Evaluation

5.1 *Evaluation environment*

One trial is performed until 2000 block heights are completed, and this is tried 10 times each with 3 types of initial mining powers (1000×100MH/sec, 5000×100MH/sec, 10000×100MH/sec).

In addition, the mining power is randomly increased or decreased according to the reality, and as an example, it is changed as shown in Fig. 4. This is an example when the original mining power is his 1000×100MH/sec, and the amount of change in the mining power is the same when he is 5000×100MH/sec and 10000×100MH/sec.

5.2 *Performance evaluation*

- Standard deviation of block generation time

Fig. 5 shows the standard deviation of the block generation time between the conventional method and the proposed method. The vertical axis shows the standard deviation of the block generation time, and the horizontal axis shows the mining power. The evaluation results showed that the standard deviation was small in all cases. From this, it showed that the variation in block generation time has become smaller. In particular, the smaller the original mining power, more effective the proposed method is.

- Average block generation time

Fig. 6 shows the average block generation time of the conventional method and the proposed method. The vertical axis shows the average block generation time, and the horizontal axis shows the mining power. For example, 1000 on the horizontal axis has an original

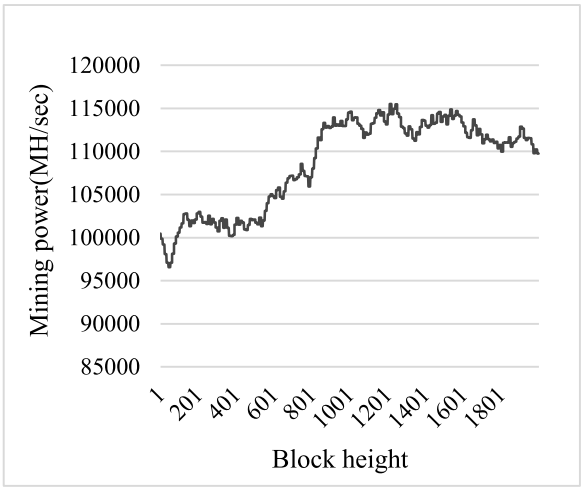

Fig. 4. Example of transition of mining power.

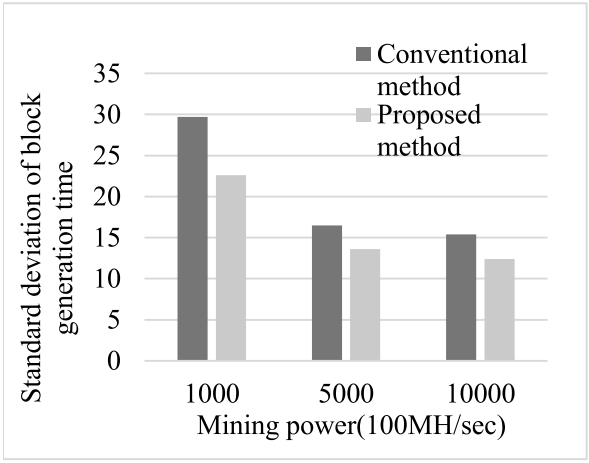

Fig. 5. Evaluation of standard deviation of block generation time.

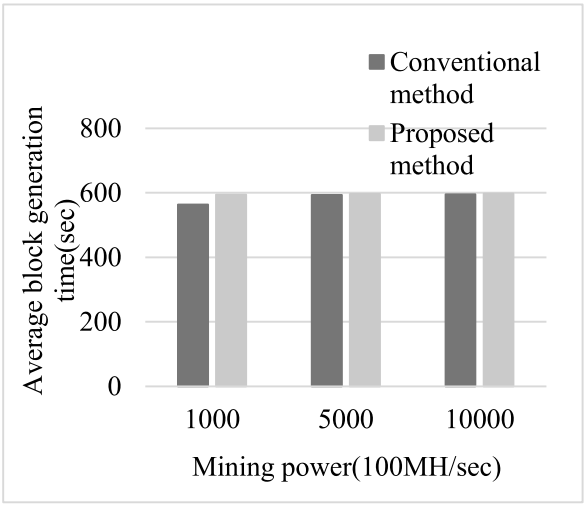

Fig. 6. Evaluation of average block generation time.

mining power of 1000×100 MH/sec. The target value here is 600 sec (10 minutes). The evaluation showed that the smaller the original mining power, the more effective the proposed method is, and the larger the original mining power is, the more the proposed method does not affect the average block generation time.

6. Consideration

The proposed method showed better results in the evaluation of the standard deviation of the block generation time regardless of the magnitude of the initial mining power. One of the reasons for this is that the change in the number of executions of the proposed method due to the difference in mining power was suppressed by changing the judgment criteria for adjusting the mining difficulty level according to the mining power. For example, if a certain standard value is set for adjusting the difficulty level of mining, the larger the mining power is, the smaller the rate of change is, and the proposed method will not be executed. Therefore, the result isn't effective. Also, the smaller the mining power, the more effective the proposed method. This shows that the proposed method is effective when the mining power changes dramatically.

The evaluation of the average block generation time showed that the smaller the mining power, the more effective the proposed method. This is because if the mining power is small, the rate of change in the whole increases when the mining power is changed. In other words, the proposed method is effective when the mining power changes dramatically. On the other hand, at 10000×100 MH/s, it was not affected much by the change in mining power, and good results were shown even with the existing method.

From this, we think that the proposed method is effective when a large-scale mining pool stops or starts mining in an actual Bitcoin blockchain network.

7. Conclusion

In recent years, research on virtual currencies and

blockchain has been actively conducted. Blockchain is a decentralized transaction ledger that does not require an administrator, and is an epoch-making technology that has merits such as keeping the value of information in a reliable state, being difficult to falsify, and reducing the cost of an administrator. However, it is said that there are still many issues. One of them is the instability of block generation time.

Currently, as a countermeasure, the mining difficulty level is adjusted once every two weeks, but even the average block generation time for two weeks is sometimes more than one minute away from the target value, so it is sufficiently stable. It cannot be said that it is.

Therefore, in order to stabilize the block generation time more than before, we considered a method to dynamically adjust the mining difficulty level by changing the mining power.

The proposed method was evaluated by the standard deviation and average of the block generation time, and when the mining power changed dramatically, the proposed method was considered to be effective. Even in the actual Bitcoin blockchain network, it is used in situations where the computing power fluctuates greatly, such as when a large-scale mining pool goes in and out, and in a system where Bitcoin becomes widespread and the transaction completion time must be constant. We thought that the proposed method was effective in the situation.

This work was partly supported by JSPS KAKENHI Grant Number JP20H00589.

References

1) S.Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System, 2008”, https://bitcoin.org/bitcoin.pdf.
2) Y.Ehara, M.Tada, “How to Secure Transparency for Random Number Generation Using Blockchain”, *Computer Security Symposium 2017 Proceedings*, **2017**[2], 915 - 922(2017).
3) “Difficulty -BTC.com”, https://btc.com/stats/diff.
4) Y.Sagami, “Optimal Mining and Hash Rate”, *The economic review of Seinan Gakuin Universiaty*, **54**[3・4], 241 - 258(2020).
5) S.Noda, K.Okumura, Y.Hashimoto, “An Economic Analysis of Difficulty Adjustment Algorithms in Proof-of-Work Blockchain Systems”, *EC '20: Proceedings of the 21st ACM Conference on Economics and Computation*, 611(2020).
6) Y.Aoki, K.Otsuki, T.Kaneko, R.Banno, K.Shudo, “SimBlock: A blockchain Network Simulator”, *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, (2019).
7) R. Banno, K.Shudo, “Simulating a Blockchain Network with SimBlock”, *Proc. 2019 IEEE Int’l Conf. on Blockchain and Cryptocurrency(IEEE ICBC 2019)*, 3 - 4(2019).