Investigating Dynamic Mining Time of Private Ethereum Blockchain on IoT Devices

Xuan Chen Kien Nguyen Hiroo Sekiya

Graduate School of Science and Engineering, Chiba University

1 Introduction

Recently, blockchain technology is integrating with many fields, including the Internet of Things (IoT). Generally, the IoT devices are considerably resource-limited to combine with blockchain. The main reason is that the IoT devices do not have enough computational power for Proof-of-Work (PoW) consensus algorithm. Specifically, they can not generate blocks in a reasonable time. Thus, the blockchain-based IoT systems either use the Proof-of-Authority (PoA) algorithm or introduce a centralized, powerful mining node for reliable block generation [1]. However, PoW has a higher security level than PoA, and other consensus algorithms [2]. Meanwhile, a centralized miner hinders the blockchain network's decentralization nature, resulting in a single point of failure (for example, failed network connection). Therefore, it is essential to explore the feasibility of PoW mining on IoT devices that become more powerful.

Ethereum is one of the most popular open-source blockchain platforms, equipped with different consensus algorithms, including PoW. The PoW implementation requires nodes on blockchain networks to solve a mathematical problem. The problem's difficulty is dynamically adjusted based on the previous mining time (i.e., in both public and private Ethereum). Consequently, the public Ethereum keeps a steady mining time when merging new computational powers. Besides, privately deployed Ethereum blockchains also benefit from this mechanism by adapting the difficulty to the device's computational power. The private blockchain is well suitable for the IoT. In [3], the authors propose a blockchain architecture for IoT device access control. The mining process is conducted in a centralized miner pool while IoT devices perform information collection. They do not participate in the blockchain network. The application still incurs the limitations mentioned above.

In this paper, we investigate the mining mechanism of the Ethereum blockchain, which can dynamically adjust the mining problem's difficulty to the IoT devices. Our contributions are:

- We demonstrate the mining process's feasibility on IoT devices (i.e., Raspberry Pi 4).
- We reveal that the mining time follows an exponential distribution after adapting to the device.

2 Ethereum Mining Process

The blockchain systems use the PoW algorithm to reach consensus by enforcing the agreement maker expending a certain amount of computational effort. The PoW implementation in Ethereum (i.e., Ethash) requires a node to solve mathematical hash problems to prove the effort. The expected amount of effort in solving the problem is controlled by a parameter named $difficulty$—the parameter value embedded in each block. Once a node finds a proper answer, it will generate a block by including the answer in the block header immediately. With a higher $difficulty$ value, the device takes more time to mine the next block.

Ethereum records the timestamps for each block. The mining time M of block N is therefore calculated as the difference duration between its previous adjacent block $N-1$. Ethereum dynamically adjusts the $difficulty$ value D_N for block N based on the previous value D_{N-1} and the mining time M as the following equation. Note that the mining process on a single node does not produce forks, thus we don't consider $(2-\frac{M}{9})$ situation for uncle blocks [4].

$$D_N = (D_{N-1} + \frac{D_{N-1}}{2048} \times max[(1-\frac{M}{9}), -99]) + 2^{\frac{N}{100000}-2} \quad (1)$$

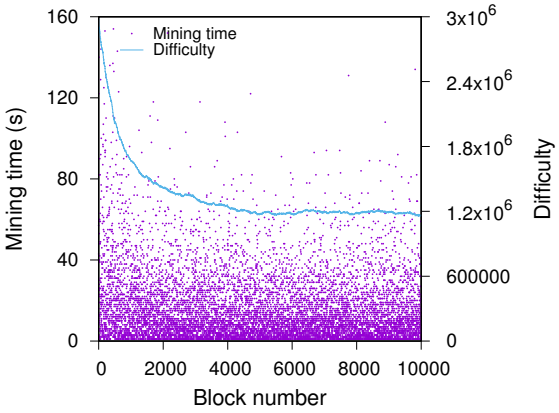
From the equation, when the block number N is below 200000, we can know that:

- If M is less than 9 seconds, D_N is adjusted upwards by $\frac{D_{N-1}}{2048}$.
- If M is within 9 to 18 seconds, D_N is left unchanged.
- If M is greater or equal to 18 seconds, D_N is adjusted downwards proportional to the timestamp difference from $\frac{D_{N-1}}{2048}$ to $99 \times \frac{D_{N-1}}{2048}$.

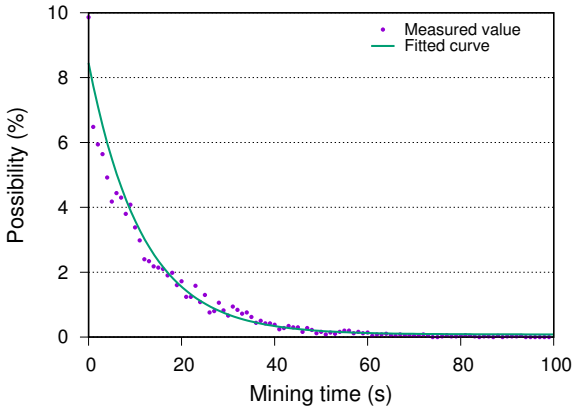
The $difficulty$ value D_N determines the general computational effort demanded to mine block $N+1$, influencing adjustment over the mining time. This mechanism can be utilized for adapting low-computational IoT devices.

3 Evaluation on IoT Device

Raspberry Pi 4 (RP4) is a latest version of open-source hardware platform Raspberry Pi. The RP de-



(a) Mining time and difficulty adjustment



(b) Exponential distribution of the mining time

図 1　Evaluation results of mining process on RP4

表 1　RP4 and Ethereum configurations

Processor	1.5 GHz 4 core ARM v8
RAM	4 GB
Disk storage	32 GB MicroSDHC
OS	Ubuntu 20.04 LTS
Ethereum	Geth 1.9.25-stable

vices are gaining popular due to their sizes, costs, and efficiency. Moreover, its capability is seemingly enough for computational tasks in IoT environments. In this work, we use a RP4 device to evaluate the mining process of private Ethereum blockchain. The configuration of RP4 and Ethereum client are listed in Table 1. In the evaluation, we deploy a private blockchain from an custom configured genesis file with an initial *difficulty* value. After that, on RP4, we start mining for over 10000 empty blocks (utilizing over an SSH connection). We interact with the blockchain network using Web3.js library and RPC communication. We write a script to automatically collect mining time and difficulty values.

The results of mining time and *difficulty* adjustment are shown in Fig. 1(a). The initial *difficulty* value keeps decreasing in the first 5000 blocks because of long mining times, which is regarded as the adjustment portion. Ethereum is adjusting its expected computational effort of mining blocks in the adjustment portion, adapting to the resource-limited device. The *difficulty* value remain at an appropriate value in the last 5000 blocks, which is regarded as the balanced portion. Blocks have different possibilities to be generated within different mining time, which follows the exponential distribution. Distinguished opportunities of each mining time lead to a dynamic balanced *difficulty* value, which follows the exponential distribution. We use a curve fitting tool (e.g., scipy.optimize package in Python3.8) to fit the posibility of each mining time from the balanced portion with equation 2. Figure 1(b) shows the fitted curve (3), which has an expected mining time of 11.07 seconds. The results indicate the feasibility of maintaining a mining node for private Ethereum blockchain on Raspberry Pi 4.

$$f(x) = \begin{cases} ae^{-\lambda x} + b & x > 0 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

$$f_{fitted}(x) = 0.0837e^{-0.0869x} + 0.0008 \tag{3}$$

4 Conclusion

This paper evaluates the difficulty adaptation mechanism in the Ethereum blockchain and the feasibility of mining on Raspberry Pi 4. We have confirmed that the difficulty value is dynamically adjusted to adapt the device, leading to proper mining time on Raspberry Pi 4. Moreover, we reveal that the mining time follows the exponential distribution after the difficulty becomes steady. The expected mining time is 11.07 seconds.

References

[1] Xuan Chen, Kien Nguyen, Hiroo Sekiya, “Characterizing Latency Performance in Private Blockchain Network ” Proc. *EAI MONAMI*, pp. 238-255, Nov. 2020.

[2] Yong Yu, Yannan Li, Junfeng Tian, Jianwei Liu, “Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things ” *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12-18, Dec. 2018.

[3] Oscar Novo, “Blockchain meets IoT: An architecture for scalable access management in IoT ” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184-1195, Apr. 2018

[4] *Geth 1.9.25-stable*, https://github.com/ethereum/go-ethereum/blob/master/consensus/ethash/consensus.go (Accessed date: January 3, 2021)