Analysis of Earned Rewards In A Blockchain with Two Selfish Miners

***Abstract*—In this paper, we study the rewards in a Proof-of-Work blockchain with two selfish miners. We analyze the rewards from both network and miner's perspectives. A simulator is implemented to study the behaviors and rewards between the miners. We first observed that the required total selfish mining rate for selfish miners to be profitable increases when the gap between the two mining rates of selfish miners decreases. When the two selfish miners have same mining rates, the required total selfish mining rate is close to 42% which is a lower bound to guarantee the profitability of selfish miners. We also compared the distributions of rewards earned by selfish miners with different mining rates. Simulations show that the strong selfish miner will be more profitable than the weak one. If the strong selfish miner has dominant mining rate, he will earn most of the rewards and the network becomes unstable. Finally, we derive an inequality to guarantee the stability of the blockchain network with two selfish miners.**

I. Introduction

Blockchain in which the transaction data are stored in a decentralized manner is the core technology used by Bitcoin [1]. The transaction data are stored in the blocks and the blocks are chained one by one using the cryptography. In a block, a hash value of previous block is appended such that the data stored in the blocks are immutable which makes the blockchain network reliable.

The hash value of previous block plays an important role in the blockchain networks. When a user node collects enough transaction data, he starts to find a nonce such that the hash value of transaction data appended with the nonce is led by a predefined number of zeros. The process of finding the nonce is called *mining* and the user node mining the block is called the *miner*. The first miner mined the next block is entitled to add the block to the blockchain and get rewards; i.e., the Bitcoins. The mechanism is called the *Proof-of-Work (PoW)* consensus mechanism.

Generally, the probability a miner mined the next block is proportional to the mining rate of a miner. The mining rate is defined as the number of nonces a miner can try during a unit time. However, a mining strategy called *selfish mining* [2] enables a miner to be more *profitabe*; that is, to earn more rewards than he would be entitled to. A miner who uses the selfish mining strategy is called a *selfish miner* while the others are called *honest miners*.

Main idea of the selfish mining is not to publish the block immediately when a selfish miner mined the next block. In this situation, only the selfish miner starts to mine the next block after his private block and other honest miners are still mined the previous one where he computation efforts of honest miners are wasted. In [2], the authors shows that selfish miner is profitable when the fraction of selfish mining rate is larger than 25%. The lowest fraction of selfish mining rate for a selfish miner to be profitable is called *profitability threshold*.

Many researches have been proposed to discuss the impact of selfish mining in PoW blockchains [3]–[19]. The enhancement, prevention, detection of selfish mining attacks are discussed in [3]–[9]. We are more interested in discussing the rewards earned by the miners. The analysis of rewards have been surveyed in [10]–[19]. The researches focus on how can each selfish miner earn more rewards by using the selfish mining strategy. However, the impact of selfish mining to the overall blockchain network and the individual miners shall be considered together.

In this paper, we discuss the earned rewards from both network and miner's perspectives. We consider the blockchain with one honest and two selfish miners. We hope to find the answers of the following two questions:

- From network's perspective, what is the profitability threshold for all selfish miners to be profitable?
- From miner's perspective, how can each miner be profitable if there are other selfish miners in the blockchain network?

We use simulations to study the behaviors and rewards of the miners in a blockchain with two selfish miners. We first found that the required total selfish mining rate for selfish miners to be profitable increases when the gap between the two mining rates of selfish miners decreases. When the two selfish miners have same mining rates, the required total selfish mining rate is close to 42% which is a lower bound to guarantee the profitability of selfish miners. We also analyze the distributions of rewards earned by selfish miners with different mining rates. Simulations show that the strong selfish miner will be more profitable than the weak one. If the strong selfish miner has dominant mining rate, he will earn most of the rewards and the blockchain becomes unstable. The threshold of the unstable situation is also derived in this paper.

The rest of this paper is organized as follows. The selfish mining strategies and the related works are described in the next section. A simulator is implemented in Section III. Simulation results are discussed in Section IV. Finally, some concluding remarks are given.

II. Selfish Mining Strategy and Related Works

The selfish mining strategy is first proposed in [2] where only a single selfish miner exists in the blockchain. In this section, we first introduce the selfish mining strategy in a blockchain with one selfish miner. Then, the selfish mining strategy is extended for multiple selfish miners.

A. One Selfish Miner

In a blockchain with one selfish miner, the other honest miners can be viewed as a single honest miner without loss of generality. Main idea of the selfish mining strategy is not to publish the block if the selfish miner mined the block first. He keeps the block in private and start to mine the next block. If his private chain is longer than the public chain,

he is guaranteed to be profitable. Details of the selfish mining strategy are as follows.

In the beginning, the honest and selfish miners compete to mine the first block. If the honest miner wins, he releases the block immediately and both miners compete to mine the next block again. However, if the selfish miner wins, he keeps the block in private and start to mine the next block. In this situation, the honest miner still mines the block which has been mined by the selfish miner. The computation efforts of honest miners are wasted.

If the selfish miner has a private block and the honest miner mined the next block, the honest miner will publish this block immediately on the public chain. The selfish miner is then notified that there is a new block added to the public chain, he will publish his private block such that the chain has two branches. When a honest miner found that there are branches from the public chain, he will randomly choose a chain to mine the next block. However, the selfish miner will only mine the next block on his branch. The chain on which the next block is first mined will be longer than the other and becomes the public chain. This is called the *longest chain rule* [1].

If the selfish miner mined the next block, he will keep the two blocks in private. If a honest miner then mined a block, the selfish miner will release his two private blocks and becomes the longest chain. If the selfish miner then mined the next block, he keeps three or more blocks in private, he remains keeping these blocks in private until the difference between the private and public chains equals to one.

In a blockchain with a selfish miner, some researches focus on how the selfish mining strategy affects the rewards of the miners [11]–[14] or network performances [10]. In [11], the authors discussed the attacks to study the winning rate and fairness of selfish mining strategy. If a miner misestimates his mining rate, the effect is discussed in [12]. In [13], [14], tame theory is employed to analyze the blockchain with selfish miningstrategy. The Bitcoin network performance is analyzed in [10].

B. Two Selfish Miners

Since selfish mining strategy enables a miner to be profitable, it is probable that multiple selfish miners may exist in the blockchain without knowing each other. In the blockchain with multiple selfish miners, each selfish miner acts independently and considers himself as the only selfish miner. We consider the blockchain with two selfish miners in this paper. The details of selfish mining strategy for two selfish miners can be found in [15]–[18]. For ease of understanding, we named the honest miner Henry and the two selfish miners Alice and Bob.

In addition to the situations in the blockchain with one selfish miner, there will be cascading actions in the blockchain with two selfish miners. One example is that Alice and Bob have two and three private blocks respectively. If Henry mined a block and add the block to public chain, Alice will release her two private blocks to become the longest chain. When Bob is notified that Alice releases her two private blocks, Bob will release his three private blocks and earn all the rewards.

In [15]–[18], the authors use simulations to analyze the blockchain with multiple selfish miners and discuss the rewards by honest miner and selfish miners in different aspects. In [15], the authors used simulations to study the net total revenue of a miner. Difficulty adjustment is considered in this paper which makes the total net revenue decreased. The impacts of strong and weak selfish miners are also studied.

In [16], the authors make two observations. They found that the reward of a selfish miner increased with the increasing mining rates of the other selfish miners. They also found that when the selfish miners have the same mining rate, the profitability threshold of each miner decreases from 25% to 21%. In [17], the authors extend their previous work [16] to multiple selfish miners. The authors show that when the number of selfish miners increases, the profitability thread decrease.

In [18], the authors considered the impact of propagation delay in a blockchain. However, the propagation delay is much less than the mining time. We ignored the impact of propagation delay in this paper. In [19], the authors proposed a Markov chain to model the blockchain with two selfish miners. Same as the previous researches, the Markov chain shows that the profitability threshold decreased to 21.48% when two selfish miners have the same mining rates.

Different from the previous researches, we consider the fractions of earned rewards from network and miner's perspectives. We not only consider the total earned rewards by selfish miners but also we discuss the rewards distribution among the all earned rewards. The observations can be used to further design the strategy for a miner to be profitable.

III. Simulations

A. Simulation Setup

Event-driven simulation is used to model the behaviors of miners in a blockchain with two selfish miners. Mining rates of one honest miner and two selfish miners are assumed to be Poisson distributed with average mining rate r_h, r_a, and r_b respectively. That is, the mining time a miner mined a block is exponentially distributed with mean value equals to reciprocal of his mining rate. Without loss of generality, we let

$$r_h + r_a + r_b = 1. \tag{1}$$

We introduce two parameters: total selfish mining rate r_s and selfish ditribution α such that

$$r_s = r_a + r_b = 1 - r_h \tag{2}$$

and

$$\begin{cases} r_a &= \alpha \times r_s \\ r_b &= (1-\alpha) \times r_s \end{cases} \tag{3}$$

In our simulations, the total selfish mining rate r_s ranges from 0.05 to 0.45. When total selfish mining rate r_s is 0.5 or larger, the selfish miner may dominate the blockchain and selfish mining strategy is no longer needed.

The selfish distribution α ranges from 0.1 to 0.5. Smaller α value means larger gap between the mining rates of two selfish miners. We called the selfish miner with less mining rate the *weak* selfish miner and the other the *strong* selfish miner. When $\alpha = 0.5$, two selfish miners have the same mining rate. When α is larger than 0.5, the situation is the same as selfish distribution $1 - \alpha$.

The rewards earned by the three miner Henry, Alice, and Bob are denoted as R_h, R_a, and R_b respectively. The sum of rewards earned by Alice and Bob $R_a + R_b$ is the total rewards earned by selfish miners, which is denoted as R_s. We

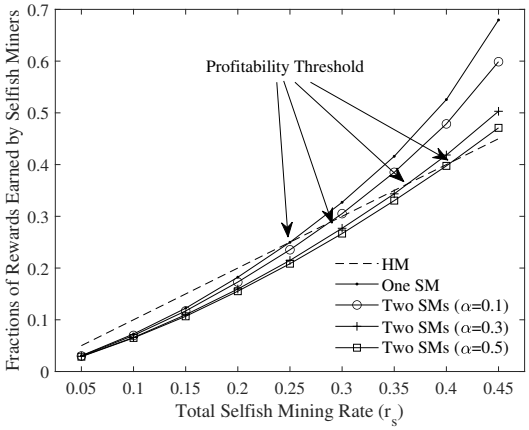

Fig. 1: Fractions of Rewards Earned by Selfish Miners

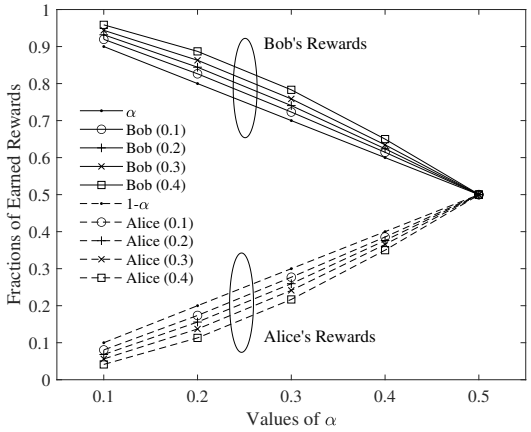

Fig. 2: Fractions of Rewards Earned by Selfish Miners

compare the R_s from different valaues of α and r_s. We also compare the rewards distribution among all selfish rewards. In our simulations, 10^7 blocks are mined in each chain and the statistics are collected from 20 blockchains.

B. Simulation Results

We first compare the total rewards earned by the selfish miners to those earned by the honest miner. Labels HM and SM in fig. 1 represent the honest miner and selfish miner. Fig. 1 shows the fractions of total rewards earned by selfish miners. From the figure, we can make the following observations:

- If only one selfish miner exists in the blockchain, the profitability threshold is about 25%, which is derived in [2]. In a blockchain with two selfish miners and the two selfish miners cooperate with each other, they are profitable when the fraction of sum of their mining rates is larger than 25%. If the two selfish miners do not cooperate with each other, the required mining rates to be profitable increased. That is, if the sum of selfish mining rates is less than 25% of all mining rates, the fraction of overall rewards earned by the selfish miners will not exceed the fraction of the selfish mining rates.
- The profitability thresholds increase when the values of α increase. In a blockchain with two selfish miners, a selfish may act as an honest miner when the other selfish miner releases his private block and create a competitive situation. That is, the selfish miner may mine the next block on the both chains of honest and selfish miners such that the overall earned rewards by the selfish miners decrease.
- When the gap between the selfish mining rates is small, the profitability threshold for the overall rewards earned by selfish miners becomes large. The largest profitability threshold occurs when the two selfish miners have same mining rates; that is, $\alpha = 0.5$. In fig.1, the profitability threshold is about 42% if both selfish miners have the same mining rates .

Next, we hope to find the rewards earned by selfish miners with different mining rates. Fig. 2 shows the ratios of rewards earned by Alice and Bob to all rewards earned by Alice and Bob. We compare the $R_a/(R_a + R_b)$ to the value of α and $R_b/(R_a + R_b)$ to the value of $1 - \alpha$. The labels in the figure represent the selfish miner with total selfish mining rate. From the figure, we can make the following observations:

- As the weak selfish miner Alice, no matter how many rewards earned by all selfish miners, the ratios of rewards earned by Alice are always less than α which is the fraction of her mining rates among all selfish mining rates. The fraction of earned rewards by strong selfish miner Bob among the rewards earned by all selfish miners is always larger than $(1 - \alpha)$ which is the fraction of Bob's mining rate.
- The gaps between the fractions of earned rewards and mining rates decrease with increasing value of α. Smaller value of α means larger gap between the mining rates of the selfish miners. In this situation, strong selfish miner will be more profitable and the reward earned by the weak selfish miner is much less than the fraction of his mining rate. When α equals to 0.5, both selfish miners earn the same amounts of rewards.
- When the value of α is fixed, it is shown that the gaps between the fractions of earned rewards and mining rates increase with increasing value of total selfish mining rate r_s. This is because when the value of r_s is large, the mining rate of strong selfish miner Bob is also large such that he is able to earn more rewards in the blockchain. When the fractions of rewards earned by Bob increase, the fraction of rewards earned by Alice decrease.

We also consider the profitability thresholds for a selfish miner. Figs. 3 and 4 show the fractions of earned rewards with different selfish mining rates. In fig. 3 we found that if the mining rate of a selfish miner is less than or equal to 0.2, the selfish miner will never be profitable no matter what the mining rate of the other selfish miner is. A special case occurs $r_a = 0.2$ and $r_b = 0.4$ where the total selfish mining rate is larger than 0.5 and most of rewards will be earned by the strong selfish miner Bob.

From fig. 4, we observed that when the selfish mining rate is larger than or equal to 0.25, the selfish miner is profitable if he has more mining rate then the other selfish miner. However, when the mining rate of the other selfish miner is larger, the fractions of rewards decrease and may be not profitable. When

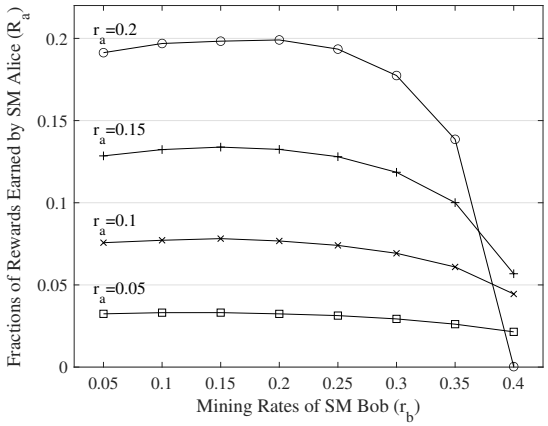

Fig. 3: Fractions of Rewards Earned by Selfish Miners with Small Mining Rates

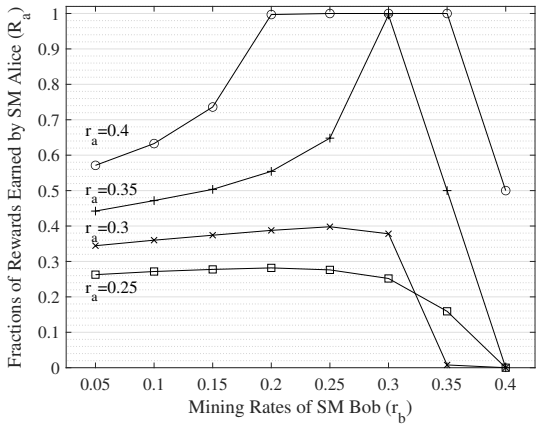

Fig. 4: Fractions of Rewards Earned by Selfish Miners with Medium or Large Mining Rates

the mining rate of a selfish miner is large enough, the earned rewards increase with the increasing other's selfish mining rates. This is because that when the other's selfish mining rates increase, the total selfish mining rate increases such that most of rewards will be earned by the strong selfish miner.

Finally, we consider the situation when the sum of selfish mining rate is large. In fig.4, when the sum of selfish mining rate r_s is larger than 0.65, the rewards will be earned by selfish miners. However, when the gap between the mining rates of two selfish miners is small, the blockchain is in an unstable situation. For example, if both miners have the same mining rate and is larger than that of honest mining rate, the blocks mined by the selfish miners will not be released and there will be no blocks in the blockchain. In such situation, the blockchain is unstable and useless. To avoid the unstable situation, we derived an inequality to calculate the threshold for a stable blockchain network.

In order to prevent the situation that a selfish miner hides their mind blocks for a long time, we let

$$r_h \geq \min(r_a, r_b). \tag{4}$$

TABLE I: Stability Threshold of r_b When r_a is Fixed

r_a	0.05	0.1	0.15	0.2	0.3	0.35	0.4	0.45
max r_b	0.5	0.5	0.5	0.5	0.4	0.325	0.3	0.275

This equation makes the weak selfish miner publish his private block.

In addition, if the mining rate of strong selfish miner is larger than the sum of mining rates from other miners, including honest and selfish miners, he will dominate the blockchain. To prevent the situation, we have

$$r_h + \min(r_a, r_b) \geq \max(r_a, r_b). \tag{5}$$

We can conclude that the following equations shall be satisfied in order to guarantee stability of the blockchain.

$$\max(r_a, r_b) \leq 1/2 \tag{6}$$

and

$$r_a + r_b \leq 1 - \min(r_a, r_b) \tag{7}$$

From fig. 4, we verify the equations (6) and (7). When the value of r_a is fixed, the maximum value of r_b is as follows.

$$r_b \leq \min(1/2, 1 - r_a - \min(r_a, r_b)) \tag{8}$$

Table I shows the threshold of r_b when the value of r_a is fixed. From Table I, figs. 4 and 3, we found that when the value of r_b is larger than the threshold, the blockchain becomes unstable.

IV. Conclusions and Future Works

In this paper, we use simulations to study the rewards earned by all miners in blockchain from both network and miner's perspectives. In addition to the results previous researchers have found, we have several interesting observations. From the network's perspective, the profitability threshold increases with the decreasing gap between the selfish mining rates. The profitability threshold for selfish miners is between the range 25% to 42%.

We also study the rewards earned by each selfish miner. Simulations show that the strong selfish miner will be more profitable than the weak one. The gaps between the earned rewards decrease with the increasing value of α and decreasing total selfish mining rates.

The conditions which a selfish miner is profitable is discussed according to the selfish mining rates r_a and r_b. When the selfish mining rate is less than 20%, it is impossible for the selfish miner to be profitable. If the selfish mining rate is larger than 25% and larger than that of the other selfish miner, he will be profitable. Otherwise, the rewards will be earned by the other selfish miner. When the selfish miners both hide their mined blocks, the network becomes unstable. In this paper, we derive an inequality to guarantee the stability of a blockchain. Correctness of the inequality for stability is also verified via simulations.

In this paper, we only discussed simulation results of the blockchains with two selfish miners. Analytical models for the blockchain system will be left for our future works. We will also extend the analysis to that with multiple selfish miners and study the behaviors and earned rewards of each miner. The results can be used to design a new mining strategy with more profitability.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[2] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 436–454.

[3] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 305–320.

[4] K. Nicolas, Y. Wang, G. C. Giakos, B. Wei, and H. Shen, "Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach," *IEEE Access*, vol. 9, pp. 3838–3857, 2021.

[5] M. J. Jeyasheela Rakkini and K. Geetha, "Comprehensive overview on the deployment of machine learning, deep learning, reinforcement learning algorithms in selfish mining attack in blockchain," in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, 2022, pp. 1–5.

[6] S.-N. Li, Z. Yang, and C. J. Tessone, "Mining blocks in a row: A statistical study of fairness in bitcoin mining," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–4.

[7] J. Lee and Y. Kim, "Preventing bitcoin selfish mining using transaction creation time," in *2018 International Conference on Software Security and Assurance (ICSSA)*, 2018, pp. 19–24.

[8] S. Reno and S. Sultana, "Preventing selfish mining in public blockchain using alarming block and block interval time approach," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2022, pp. 988–993.

[9] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 360–364.

[10] S. G. Motlagh, J. Mišić, and V. B. Mišić, "The impact of selfish mining on bitcoin network performance," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 724–735, 2021.

[11] Y.-F. Wen and C.-Y. Huang, "Exploration of mined block temporarily holding and enforce fork attacks by selfish mining pool in proof-of-work blockchain systems," *IEEE Access*, vol. 10, pp. 61 159–61 174, 2022.

[12] S.-Y. Chang, "Mining power misestimation in pow blockchain," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2020, pp. 148–152.

[13] B. Jebari, K. Ibrahimi, M. Jouhari, and M. Ghogho, "Analysis of blockchain selfish mining: a stochastic game approach," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 4217–4222.

[14] K. R and K. M. Pitchai, "Modeling and simulation of selfish mining attacks in blockchain network using evolutionary game theory," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2023, pp. 1016–1021.

[15] H. Azimy and A. Ghorbani, "Competitive selfish mining," in *2019 17th International Conference on Privacy, Security and Trust (PST)*, 2019, pp. 1–8.

[16] S. Zhang, K. Zhang, and B. Kemme, "A simulation-based analysis of multiplayer selfish mining," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–5.

[17] ——, "Analysing the benefit of selfish mining with multiple players," in *2020 IEEE International Conference on Blockchain (Blockchain)*, 2020, pp. 36–44.

[18] Q. Xia, W. Dou, T. Xi, J. Zeng, F. Zhang, J. Wei, and G. Liang, "The impact analysis of multiple miners and propagation delay on selfish mining," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2021, pp. 694–703.

[19] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, "A deep dive into blockchain selfish mining," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.