Research and Analysis of Mining Pool Selection Strategies in Blockchain (Postprint)

Authors: Di Jian, Lin Weihua

Date: 2019-05-10T00:00:00+00:00

Abstract

In blockchain networks based on Proof of Work (PoW), miners typically choose to join mining pools. Since multiple mining pools exist with varying hash power and may adopt different reward mechanisms, miners can obtain different returns from different pools. To address the mining pool selection problem faced by miners, a mining pool selection model based on risk decision criteria is established, investigating the impact of pool hash power and reward mechanisms on miners' optimal selection strategies. First, miners' returns in different pools are calculated to present a payoff matrix; second, optimal selection strategies are derived using the maximum likelihood criterion and the expected value criterion, respectively; finally, the proposed strategies are validated and analyzed through simulation experiments. Experimental results demonstrate that, compared with simple strategies, the proposed strategies can yield higher returns for miners in the vast majority of cases.

Full Text

Preamble

Vol. 37 No. 6
Application Research of Computers
ChinaXiv Cooperative Journal

Research and Analysis of Mining Pool Selection Strategy in Blockchain

Di Jian, Lin Weihua†
(School of Control & Computer Engineering, North China Electric Power University, Baoding, Hebei 071003, China)

Abstract: In blockchain networks based on Proof of Work (PoW), miners typically choose to join mining pools. Since multiple pools exist with varying com-

puting power and may adopt different reward mechanisms, miners can obtain different rewards from different pools. To address the pool selection problem faced by miners, this paper establishes a pool selection model based on risk decision criteria and investigates how pool computing power and reward mechanisms affect miners' optimal selection strategies. First, we calculate miners' rewards in different pools and present a reward matrix. Second, we derive optimal selection strategies using both the maximum likelihood criterion and the expected value criterion. Finally, we validate and analyze the proposed strategies through simulation experiments. Experimental results demonstrate that compared with simple strategies, the proposed strategy yields higher rewards for miners in most cases.

Keywords: bitcoin; blockchain; mining pool; reward system; risk decision

0 Introduction

Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008 [1], blockchain technology has attracted increasing attention. Its main characteristics include decentralization, trustlessness, collective maintenance, security, and immutability [2]. Due to these features, blockchain technology can be applied in numerous fields such as finance, energy internet, and information security [3–6]. As a typical application of blockchain technology, the Bitcoin system utilizes a Proof of Work (PoW) consensus mechanism [7] to achieve transaction immutability and unforgeability. In the Bitcoin system, mining refers to the process where all participants contribute their computing power to solve a mathematically difficult problem with dynamically adjustable difficulty, seeking a qualifying random value to generate new blocks. These participants are called miners.

If a miner successfully discovers a block, they receive the block reward as compensation for their contributed computing power. The mining difficulty automatically adjusts based on how easily the system currently generates blocks, typically set to produce one block every ten minutes. In practice, due to the enormous computing power in the current Bitcoin system, the probability of an independent miner discovering a new block is essentially zero [8]. Therefore, miners usually choose to join mining pools to improve revenue stability, while pools can adopt arbitrary mining strategies [9].

A mining pool typically consists of an administrator and multiple miners. Regardless of which miner in the pool discovers a new block, the reward is distributed among all miners in the pool according to their contribution ratio. Since generating a full Proof of Work is extremely difficult, the administrator typically sets a less difficult mathematical problem for each miner and requires them to submit solutions—satisfying random values known as partial Proof of Work.

Currently, pool reward distribution systems [10] mainly include three types: Proportional, Pay-per-share (PPS), and Pay-per-last-N-shares (PPLNS). The first two are collectively called simple methods. The Proportional method distributes rewards to miners based on their contributed computing power when the pool discovers a new block. The PPS method differs only in that it distributes rewards based on miners' contributions regardless of whether the pool currently discovers new blocks. The PPLNS mechanism distributes the pool' s rewards equally among the most recently submitted N partial Proof of Work after several rounds.

Regarding pool selection strategies, existing research includes: Reference [11] studied the impact of computing power and network latency on pool selection strategies and established an evolutionary game model to analyze these factors' influence. Reference [12] investigated different reward distribution mechanisms and how N in the PPLNS mechanism affects miner rewards. However, [12] only examined the impact of different reward distribution systems in independent pools on miner rewards, whereas in reality, multiple competing pools typically exist in a blockchain network. Building upon this, our paper studies the impact of competing pools' computing power and different reward distribution mechanisms on pool selection strategies, proposing a novel pool selection strategy.

---

1 Mining Pool Selection Strategy

This chapter assumes a scenario in a blockchain network where the total network computing power is 1, and only two pools, A and B, exist. Both pools conduct honest mining without launching any attacks [13,14]. Pool A adopts the Proportional reward distribution system with computing power α, while pool B adopts the PPLNS reward system with computing power β, where $\alpha + \beta = 1$. In the PPLNS system, we assume each round contains M partial Proof of Work, and a miner' s submitted partial Proof of Work has a random position in M with probability $1/M$. The position is also random across different rounds. We further assume that mining difficulty D and block reward R remain constant in each round, round duration T is constant, and for this study, we do not consider pool fees—pools distribute all block rewards to miners.

1.1 Pool Revenue

Generally, miners with greater computing power have higher probabilities of discovering new blocks. As shown in [1], the block mining process approximates a Poisson distribution, where blocks are mined independently at a constant probability under fixed computing power. According to [10], the expected number of blocks mined by a node with computing power H in time period t is $\frac{Ht}{2^{32}D}$, and the expected reward is $\frac{HtR}{2^{32}D}$.

1.2 Maximum Expected Value Criterion

The principle of the maximum expected value criterion is as follows: Assume the probability of each event occurring is p_j, and the profit/loss value (i.e., the element representing the "strategy-event" pair in the reward matrix) when adopting strategy i under event j is denoted as a_{ij}. Then the expected reward for each strategy is:

$$E_i = \sum_{j=1}^{n} p_j a_{ij}$$

where m represents the number of adoptable strategies (number of schemes), and n represents the number of possible events (number of states), with $\sum_{j=1}^{n} p_j = 1$. The decision criterion selects the maximum value from these expected rewards, and its corresponding strategy is the optimal strategy.

Applying this principle, let $E(A)$ and $E(B)$ represent the expected reward values for pools A and B, respectively. From Table 1 , we obtain:

$$E(A) = \frac{1}{M} \cdot \frac{KR\alpha}{M} + \frac{M-1}{M} \cdot \frac{KR\alpha}{M} = \frac{KR\alpha}{M}$$

$$E(B) = \frac{1}{M} \cdot \frac{KR(1-\alpha)}{MN} + \frac{M-1}{M} \cdot \frac{KR(1-\alpha)}{MN} = \frac{KR(1-\alpha)}{MN}$$

The difference is:

$$E(A) - E(B) = \frac{KR}{M}\left(\alpha - \frac{1-\alpha}{N}\right) = \frac{KR}{M} \cdot \frac{N\alpha + \alpha - 1}{N}$$

Since $0 < \alpha < 1$, when $N\alpha + \alpha - 1 < 0$, i.e., $\alpha < \frac{1}{N+1}$, we have $E(A) < E(B)$, and pool B should be selected. When $\alpha > \frac{1}{N+1}$, we have $E(A) > E(B)$, and pool A should be selected. When $\alpha = \frac{1}{N+1}$, $E(A) = E(B)$, and both pools are optimal strategies.

In K rounds containing KT time units, the number of blocks mined by pools A and B in KT time are $K\alpha$ and $K(1-\alpha)$, respectively. Clearly, the variance of pool A is zero, making its expected reward value more stable, meaning pool A is the optimal strategy.

1.3 Maximum Likelihood Criterion

Case 1: Miner submits one partial Proof of Work per round

The reward for each partial Proof of Work in pool A is $\frac{KR\alpha}{M}$, and in pool B is $\frac{KR(1-\alpha)}{MN}$. Therefore, the miner' s reward is $\frac{KR\alpha}{M}$ in pool A. In pool B, if the

submitted partial Proof of Work is among the most recent N shares, the reward is $\frac{KR(1-\alpha)}{N}$; otherwise, it is 0.

There are KM partial Proof of Work in K rounds. According to [12], we can derive the miner' s reward matrix as shown in Table 1.

Table 1: Miner' s Reward Matrix 1

According to the maximum likelihood criterion, when $\frac{M-j}{M} > \frac{j}{M}$, i.e., $j < \frac{M}{2}$, state s_1 is considered to occur, and pool A should be selected; otherwise, pool B should be selected. When $j = \frac{M}{2}$, both pools A and B are optimal strategies.

Theorem 1: When $\alpha < \frac{1}{2}$, pool B is the optimal strategy; when $\alpha > \frac{1}{2}$, pool A is the optimal strategy; when $\alpha = \frac{1}{2}$, both pools A and B are optimal strategies. If $N < M$, then when $\frac{N}{M} > \frac{1}{2}$, the optimal strategy is pool A; when $\frac{N}{M} < \frac{1}{2}$, the optimal strategy is pool B; when $\frac{N}{M} = \frac{1}{2}$, both pools A and B are optimal strategies.

When $\alpha > \frac{1}{2}$, $R_1 > 0$ always holds, so pool A should be selected. When $\alpha < \frac{1}{2}$, we need to further calculate the value of R_1 to make the corresponding selection.

Case 2: Miner submits multiple partial Proof of Work per round

Assume a miner can submit multiple partial Proof of Work per round. For simplicity, this paper studies the case where a miner can submit two partial Proof of Work per round, and these two submissions have adjacent positions. We analyze this using the maximum likelihood criterion. From [12], the reward matrix is as shown in Table 5 .

Table 5: Miner' s Reward Matrix 2

According to the maximum likelihood criterion:

When $j \leq \frac{M}{2}$, state s_1 occurs, and pool A should be selected. When $j > \frac{M}{2}$, state s_3 occurs, and pool B should be selected. If $j = \frac{M}{2}$, both pools A and B are optimal strategies.

When $\alpha > \frac{1}{2}$, $R_2 < 0$ always holds, so pool A should be selected. When $\alpha < \frac{1}{2}$, we need to further calculate the value of R_2 to make the corresponding selection.

Theorem 2: When $\alpha > \frac{1}{2}$, pool A is the optimal strategy; when $\alpha < \frac{1}{2}$, pool B is the optimal strategy; when $\alpha = \frac{1}{2}$, both pools A and B are optimal strategies. If $N < M$, then when $\frac{N}{M} > \frac{1}{2}$, the optimal strategy is pool A; when $\frac{N}{M} < \frac{1}{2}$, the optimal strategy is pool B; when $\frac{N}{M} = \frac{1}{2}$, both pools A and B are optimal strategies.

From Theorems 1 and 2, the optimal pool selection strategies are identical in the two scenarios discussed above, so detailed examples are omitted here.

---

2 Simulation and Analysis

This chapter evaluates the proposed pool selection strategy. To better demonstrate the advantages of our strategy, we conduct comparative experiments: always selecting pool A is called Strategy A, always selecting pool B is called Strategy B, and our proposed strategy is called the New Strategy. Based on the previous discussion, the strategy derived using the maximum expected value criterion essentially means selecting the pool with greater computing power can increase miners' expected rewards. When pools A and B have equal computing power, the choice is obvious—pool A should be selected because its revenue stability is better. To intuitively verify the effectiveness of the strategy derived using the maximum likelihood criterion, we conduct the following experiments.

The experiments use the Monte Carlo method to simulate the mining process, implemented in Python, primarily utilizing the Numpy scientific computing library and Matplotlib plotting library. Numpy performs the simulation experiments, while Matplotlib visualizes the results. Experimental environment: Windows 7 64-bit system, Python 3.6.

The experimental scenario involves two pools, A and B, in a blockchain network with computing powers α and β, respectively. Pool A adopts the Proportional reward distribution mechanism, while pool B adopts PPLNS. As discussed in Section 1.3, the optimal strategies for submitting one or two partial Proof of Work per round are identical. Therefore, for simplicity, this experiment assumes each miner can only submit one partial Proof of Work per round, and both pools A and B receive five partial Proof of Work per round. Pool B distributes rewards every three rounds, so possible values for N are $\{1, 2, ..., 15\}$. The position of the miner' s submitted partial Proof of Work among all submissions is represented by j, where $1 \leq j \leq 5$.

2.2 Results Analysis

For each possible value of N, we conduct 1,000 experiments. Figure 1 [Figure 1: see original paper] shows the distribution of counts for the five possible positions of the miner' s submitted partial Proof of Work for each N. Since submission positions are equally probable, we observe approximately 200 submissions per position. For each N, there are two states s_1 and s_2. Figure 2 [Figure 2: see original paper] shows the counts for these two states across 1,000 experiments for each N.

Figures 3 [Figure 3: see original paper] through 5 [Figure 5: see original paper] show the optimal selection strategies when pools A and B have different computing powers. We can see that for the same N value, the optimal selection strategy changes according to the different computing powers of pools A and B. When pool computing power is fixed, the optimal selection strategy is also influenced by the value of N.

We can conclude: When $\alpha = 0.45, \beta = 0.55$, for $N = \{1, 2, 8\}$, the miner' s

optimal strategy is to select pool A; for $N = \{3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$, the miner' s optimal strategy is to select pool B.

When $\alpha = \beta = 0.5$, for $N = \{1, 2, 6, 7, 11, 12\}$, the optimal strategy is pool A; for $N = \{3, 4, 8, 9, 13, 14\}$, the miner' s optimal strategy is to select pool B; for $N = \{5, 10, 15\}$, both pools A and B are optimal strategies.

When $\alpha = 0.55, \beta = 0.45$, for $N = \{3, 4, 8\}$, the miner' s optimal strategy is to select pool B; for $N = \{1, 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$, the miner' s optimal strategy is to select pool A.

By comparing the rewards miners obtain using the New Strategy versus Strategies A and B across 1,000 experiments, we can determine the counts where $R(\text{New}) < R(A)$, $R(\text{New}) > R(A)$ and $R(\text{New}) < R(B)$, and $R(\text{New}) \geq R(B)$, as shown in Figures 6 [Figure 6: see original paper] through 8 [Figure 8: see original paper]. For the three different pool computing power scenarios and any N, miners using the New Strategy obtain higher rewards than using single Strategies A or B in the vast majority of the 1,000 experiments, demonstrating that the New Strategy is superior to single strategies.

---

3 Conclusion

This paper studied the problem of mining pool selection in blockchain networks. Considering the impact of competing pools with different reward distribution systems on miner rewards, we conducted research and analysis using both the maximum likelihood criterion and the maximum expected value criterion, providing optimal selection strategies for different pool computing powers. We also designed corresponding experiments to evaluate the proposed pool selection strategy, and experimental results demonstrated its effectiveness.

However, this research has limitations: it does not consider factors such as different numbers of Proof of Work received by pools in a round, nor situations where pool computing power is not constant.

To address these unresolved issues, we propose potential solutions: In a round, the number of Proof of Work generated in a pool depends only on node computing power and partial Proof of Work difficulty. Assuming the total computing power of the entire blockchain network remains constant, we can set two parameters $\varepsilon_1, \varepsilon_2$ to represent migration rates between the two pools. Based on computing power and partial Proof of Work difficulty, we can determine the number of partial Proof of Work generated per unit time. Since the Proof of Work generation process is a random process, we can use the Monte Carlo method to simulate the mining process and analyze it using risk decision methods.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008) [2018-9-13]. https://bitcoin.org/bitcoin.pdf.

[2] Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends [J]. *Acta Automatica Sinica*, 2016, 42(4): 481-494.

[3] Li Dong, Wei Jinwu. Theory, application fields and challenge of the blockchain technology [J]. *Telecommunications Science*, 2016, 32(12): 20-25.

[4] Eyal I. Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities [J]. *Computer*, 2017, 50(9): 38-49.

[5] Zhu Liehuang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology [J]. *Journal of Computer Research and Development*, 2017, 54(10): 2170-2186.

[6] Liu Aodi, Du Xuehui, Wang Na, et al. Research progress of blockchain technology and its application in information security [J]. *Journal of Software*, 2018, 29(7): 2092-2115.

[7] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications [C]// Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 281-310.

[8] Lewenberg Y, Bachrach Y, Sompolinsky Y, et al. Bitcoin mining pools: a cooperative game theoretic analysis [C]// Proc of the 14th International Conference on Autonomous Agents and Multiagent Systems. Richland: IFAAMAS, 2015: 919-927.

[9] Fisch B, Pass R, Shelat A. Socially optimal mining pools [C]// Proc of the 13th International Conference on Web and Internet Economics. Berlin: Springer, 2017: 205-218.

[10] Rosenfeld M. Analysis of Bitcoin pooled mining reward systems [EB/OL]. (2011) [2018-10-23]. https://arxiv.org/abs/1112.4980.

[11] Liu Xiaojun, Wang Wenbo, Niyato D, et al. Evolutionary game for mining pool selection in blockchain networks [J]. *IEEE Wireless Communications Letters*, 2017, 7(5): 760-763.

[12] Qin Rui, Yuan Yong, Wang Feiyue. Research on the selection strategies of blockchain mining pools [J]. *IEEE Trans on Computational Social Systems*, 2018, 5(3): 748-757.

[13] Eyal I. The miner' s dilemma [C]// Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2015: 89-103.

[14] Luu L, Saha R, Parameshwaran I, et al. On power splitting games in distributed computation: the case of bitcoin pooled mining [C]// Proc of the 28th

IEEE Computer Security Foundations Symposium, Piscataway, NJ: IEEE Press, 2015: 397-411.

[15] Heilman E. One weird trick to stop selfish miners: fresh bitcoins, a solution for the honest miner (poster abstract) [C]// Proc of International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 161-162.

Note: Figure translations are in progress. See original paper for figures.