Hindawi
Security and Communication Networks
Volume 2022, Article ID 8265140, 10 pages
https://doi.org/10.1155/2022/8265140

Research Article

Selection Strategy of Mining Pool under Various Different Payment Mechanisms

Tan Xing-Hong,[1] **Fu Lu-Xia**,[1] **Zhang Zhuang**,[1] **and Tan Liang**[1,2]

[1]*College of Computer Science, Sichuan Normal University, Chengdu, Sichuan 610101, China*
[2]*Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China*

Correspondence should be addressed to Tan Liang; jkxy_tl@sicnu.edu.cn

Received 6 May 2022; Accepted 7 June 2022; Published 6 July 2022

Academic Editor: Jiewu Leng

Blockchain is becoming increasingly popular and has received extensive attention in various fields. In a proof-of-work-based blockchain, miners usually choose to join a mining pool for mining to gain revenue. Different mining pools may use other payment mechanisms, and each miner can earn different revenues in different pools. There are currently four common payment mechanisms used by mining pools to distribute mining revenue, namely, PPS, PPLNS, PPS+, and FPPS, and there are no relevant research results on the selection strategies of these four payment mechanisms. To this end, this paper models the pool selection problem as a risky decision problem and proposes the selection strategies of these four mining pool payment mechanisms. Firstly, miners' income under the four payment mechanisms is given; then, a mining pool selection strategy based on the change of computing power is constructed based on the Laplace criterion; finally, the proposed strategy is verified and analyzed by simulation. The experiments show that the proposed mining pool selection strategy is effective. The results of this paper can provide an essential reference for miners when making pool selection decisions.

1. Introduction

In 2008, Satoshi Nakamoto published a white paper on Bitcoin [1]. Following this, blockchain technology is becoming increasingly popular and attracting wide attention in various fields [2–6]. Due to its decentralized, de-trusted, collectively maintained, and tamper-evident properties [7], blockchain technology has been used in several areas such as medical information security management [8], smart city [9, 10], smart manufacturing [11, 12], access control framework system [13], and trusted service mechanism [14]. Bitcoin is a typical application of blockchain technology. Bitcoin mining is the process of obtaining Bitcoins, which is based on the principle of using computer computing power to solve cryptographic puzzles and use this to generate blocks that are eventually rewarded without blocks of Bitcoins. In a proof-of-work-based blockchain network, miners participate in solving a mathematical puzzle by contributing their computing power. If they are able to arrive at a solution that satisfies the practical block difficulty of the blockchain network, they are considered to have found a new block. They are rewarded for their contribution of their computing power [15]. We call the solution to a mathematical puzzle that satisfies the difficulty of generating a new block a full workload proof. For miners, solving a full workload proof alone is very difficult due to the sheer amount of computing power on the blockchain network, and to improve the efficiency of the solution, miners usually join the mining pool and contribute their computing power as a way to improve the stability of their revenue. The pool administrator, on the other hand, usually divides the mathematical puzzle that satisfies the difficulty of generating a new block into multiple less difficult mathematical problems and asks the miners in the pool to submit a solution to this less difficult mathematical problem, which is usually referred to as a partial workload proof [16]. When a miner in the pool obtains and submits a solution as a full workload proof during the calculation process, the pool is considered to have mined a

new block, and the block reward will be settled to the corresponding miner in the pool in accordance with the pool's payment mechanism. In practice, the issue of pool selection is actually the first problem miners face in pool mining, and for miners in a pool, the payment mechanism used by the pool has a significant impact on their earnings. For example, in the article [17], during the selection process of two payment mechanism mining pools, PPS and PPLNS, the PPLNS pool is settled according to the last N partial workload proofs submitted by miners, and the change of N leads to the shift of miners for the pool selection.

We perform a revenue analysis of four common mechanisms commonly used by mining pools in practice, PPS, PPLNS, PPS+, and FPPS [18–22]. We refer to the revenue generated by the packaging transaction when a block is generated as the miner's fee, and the PPS mining pool deducts the theoretical income from the mining fee and proceeds the income settlement according to the proportion of miners' calculation power in the mining pool. PPLNS mine pool will make a settlement with the miners who have recently submitted N partial proof of work after deducting the mining fee from the aggregate of the actual block production reward of the mining pool after several rounds. The PPS + mining pool mechanism combines PPS and PPLNS payment modes. The block payment reward is settled according to PPS and the number of blocks produced by the mining pool theory. The miner's fee is settled based on the actual mining fee produced by the mining pool and N partial workload proofs submitted by miners recently. The FPPS mining pool mechanism is also known as full PPS, where the pool's block rewards and miner fees are settled according to the PPS model. There are already research results comparing the PPS and PPLNS, PROP, and PPLNS payment mechanisms in the context of independent mining pools adopting different reward distribution systems. The PROP mechanism is based on the principle that when a mining pool finds a new block, it allocates a corresponding amount of revenue to the miner according to the amount of computing power he has contributed to the pool. The only difference between the principle of the PPS mechanism and PROP is that in PPS, the payout is distributed according to the size of the miner's contribution, regardless of whether or not the current pool has found a new block. Article [17] models the pool selection problem faced by miners in the case of two payment mechanisms, PPS and PPLNS, as a risky decision problem based on the maximum likelihood criterion, based on the phenomenon that miners have different returns for selecting pools with varying mechanisms of reward, and investigates the impact of the variation of N in the PPLNS mechanism on miners' optimal pool selection decision, with N referring to the number of partial workload proofs taken at the end of each settlement in the PPLNS mechanism. The article [16], on the other hand, addresses the pool selection problem faced by miners under the competitive relationship between two payment mechanisms, PROP and PPLNS, and builds a pool selection model based on the risk decision criterion, calculating the miners' returns in different pools. And the article derives the optimal selection strategy using the maximum likelihood criterion and the expected value criterion, respectively. It investigates the influence of pool computing power and reward mechanism on the miners' optimal selection strategy.

This paper aims to conduct a comparative analysis of four payment mechanisms for Bitcoin mining, model the problem of choosing a mining pool under the four payment mechanisms faced by miners as a risky decision problem, and construct a pool selection model based on Laplace's criterion. This study focuses on the pool selection of four common mining pool payment mechanisms, PPS, PPLNS, PPS+, and FPPS, in the same blockchain network competing for computing power resources, highlighting the impact of computing power allocation on pool selection. Unfortunately, the starting point of this study is different from other mine pool selection strategy papers, so it is not compared with the results of the papers with other selection strategies. The relevant selection strategy research article [16, 17] focuses on selecting the mine pool strategy under N change in the PPLNS mechanism. Still, our study focuses more on the influence of computing power distribution change. We regard the change of N as an equal possibility value. The miners who chose the PPLNS payment mechanism submitted only two results: the proof of work falling into the value range of N or not falling into the value range of N. We highlight the influence of the computing power distribution change on the choice of the four mine pool strategies. The results of this paper can provide an essential reference for miners when making pool selection decisions. Using computational experiments, we validate the effectiveness of our proposed mining pool selection strategy.

2. Related Work

The purpose of the study of mining pool strategies is to improve miners' profitability. Currently, there are several mining pools in the market. Different pools have the different computing powers and may adopt different payment mechanisms, which leads to the fact that miners cannot get the same profit from different pools. Research on mining pool strategies has produced several results in mining pool incentive strategies, mining pool attack-defense strategies, and mining pool selection strategies.

First, in terms of incentive strategies for mining pools, articles [15, 23, 24] aim to encourage honest mining, reduce the waste of computational resources due to miners' malicious behavior, and address the problems of inefficient mining and unfair returns by providing miners with a game to think about to encourage honest and cooperative mining to improve returns. In paper [25, 26], mining strategies that can improve the profits and reduce dishonest miners' profits are proposed to enhance the overall mining profits of the mining pool.

Secondly, in terms of mining pool attack and defense strategies, the article [27, 28] defines and analyzes the game theory problem of the prisoner's dilemma arising from a mining pool attack, uses the results of the congestion game to establish a pure Nash equilibrium, gives an efficient

algorithm for finding such an equilibrium, and calculates the miner's gain in the case of a mining pool attack. Articles [29–31] address the problem that miners will choose to attack each other due to the pursuit of superior strategies and high returns. By building a model of mining pool defense strategy and comparing the expected cooperative returns with attack returns, they reduce the wastage of computing power and the phenomenon of driving down mining returns caused by miners when conducting attacks, promote the cooperation of miners, and ensure stable returns of mining pools. The article [32] designs a new blockchain and provides a trust model for it to address the problem of internal attacks on mining pools. Articles [33–35] then provide mining pool attack strategies to show the vulnerability of existing mining pool structures, with the intention of deciphering the problem of the miner's prisoner's dilemma and providing advice to miners when choosing to attack or cooperate.

Finally, in terms of pool selection strategies, articles [16, 17, 36, 37] investigate how miners choose pools in blockchain networks under the influence of different block mining strategies, reward allocation mechanisms, computing power, and latency, and use pool selection strategies to obtain the best returns.

There has been a lot of research and research findings on mining pool incentive strategies, attack and defense strategies, and selection strategies. However, there is a lack of research in the literature on pool selection strategies for multiple different payment mechanisms, so there is some value in this study [38–41].

3. Mining Pool Selection Strategies

3.1. Four Mining Pool Payment Mechanisms and Miner's Earnings. A comparison of the four mining pool payment mechanisms is shown in Table 1.

The mining fee is the fee charged by a mining pool for conducting mining, usually expressed as δ. The miner's fee is the transaction fee for all transactions obtained by packing this block, in addition to the block reward. The lucky value is the ratio of the pool's actual block yield to the theoretical block yield.

$$\text{Lucky Valu} = \frac{\text{Actual Benefits}}{\text{Throretical Benefits}} \times 100\%. \tag{1}$$

For the purposes of this paper, we assume that all four pools receive a fixed miner's fee of φ per block packed. In this paper, we assume that the lucky value of mining is 100%; i.e., the expected revenue on blocks is equal to the actual return on blocks. Suppose there are a total of four mining pools V_1, V_2, V_3, and V_4 on the blockchain network, taking PPS, PPLNS, PPS+, PPS+, and FPPS payment mechanisms, respectively, with each payment mechanism accounting for e_1, e_2, e_3, and e_4 of the blockchain network's computing power, respectively, then $e_1 + e_2 + e_3 + e_4 = 1$. Assume that the blockchain network is a round from the start of mining new blocks to the end of blocking, and that each round of blocking lasts for a fixed time T, for a total of K rounds. The blockchain network has a fixed total block reward of R for each round. Total mining revenue per mining pool for round

Table 1: Comparison of four common mining pool payment mechanisms.

Payment mechanisms	Block rewards	Miners' fees	Supported mining pools
PPS	Theoretical value	No distribution	ViaBTC
PPLNS	Actual value	Actual value	AntPool, ViaBTC
PPS+	Theoretical value	Actual value	AntPool, F2Pool
FPPS	Theoretical value	Theoretical value	BTC.com

K is $S = e_i KR$, $i = \{1, 2, 3, 4\}$. Assume that each pool miner fee K round of total revenue is $S_c = K\varphi$. Assume that each pool has exactly M partial workload proofs per round, and for ease of calculation, assume that each miner provides only one partial workload proof per round, and that the position of the partial workload proof submitted by the miner among the M partial workload proofs is random and this position is the same in K rounds, and let the probability that the partial workload proof submitted by the miner in each round is at position i be p_i, $p_i = (1/M)$.

3.1.1. PPS (Pay per Share). PPS payment mechanism of the pool is based on the miner's computing power in the pool; an estimate of the daily output can be obtained in the pool, not to allocate the miner's fee; the pool will retain δ percentage of mining fees.

The mining pool that chooses the PPS payment mechanism for mining is defined as event V_1. The mining revenue for miners in event V_1 is

$$v_1 = \frac{1}{M} e_1 (1 - \delta) KR. \tag{2}$$

Since the model does not calculate miner's fees, the miner's gain in miner's fees in event V_1 is

$$S_c(v_1) = 0. \tag{3}$$

3.1.2. PPLNS (Pay per Last N Shares). The PPLNS payment mechanism mining pool will settle with the miner who submitted the last N partial workload proofs after several rounds by adding up the actual block bonus of this pool with the actual miner's fee, minus the mining fees. The revenue will be allocated to the miner who submits the last N partial workload proofs, as shown in the literature [17], $N = (k-1)M + j, k \in [1, K], j \in [1, M]$, where k refers to the number of rounds N contains and j refers to the number of partial workload proofs that N contains when a full round is not included.

The mining pool that chooses the PPLNS payment mechanism for mining is defined as event V_2, in which miners have two revenue states a and b.

In state a, the probability that some of the workload proofs submitted by miners at the settlement of each reward do not all fall within the last N candidates is

$$p_{2,a} = \frac{M-j}{M}. \tag{4}$$

The miner's mining revenue in state a of event V_2 is

$$v_{2,a} = \frac{k-1}{N} e_2 (1-\delta) KR. \tag{5}$$

The miner's gain in miner's fee for state a of event V_2 is

$$S_c\left(v_{2,a}\right) = \frac{k-1}{N} (1-\delta) K\varphi. \tag{6}$$

In state b, some of the workload proofs submitted by miners at each settlement of the reward fall within the last N candidates with the probability are

$$p_{2,b} = \frac{j}{M}. \tag{7}$$

The mining revenue of the miner in state b of event V_2 is

$$v_{2,b} = \frac{k}{N} e_2 (1-\delta) KR. \tag{8}$$

The miner's gain in miner's fee for state b of event V_2 is

$$S_c\left(v_{2,b}\right) = \frac{k}{N} (1-\delta) K\varphi. \tag{9}$$

3.1.3. PPS+ (Pay per Shares plus). The PPS + payment mechanism pool combines both PPS and PPLNS models, with PPS settling the pool's theoretical block, payout rewards, and PPLNS determining the miners' fees generated by the pool's actual block payouts.

The mining pool that chooses the PPS + payment mechanism for mining is defined as event V_3, and from Sections 3.1.2 and 3.1.3, the mining returns of miners in event V_3 are

$$\begin{aligned} v_{3,a} &= \frac{1}{M} e_3 (1-\delta) KR \ , \ p_{3,a} = \frac{M-j}{M}, \\ v_{3,b} &= \frac{1}{M} e_3 (1-\delta) KR \ , \ p_{3,b} = \frac{j}{M}. \end{aligned} \tag{10}$$

The miner's gains from the miner's fees in event V_3 were

$$\begin{aligned} S_c\left(v_{3,a}\right) &= \frac{k-1}{N} (1-\delta) K\varphi \ , \ p_{3,a} = \frac{M-j}{M}, \\ S_c\left(v_{3,b}\right) &= \frac{k}{N} (1-\delta) K\varphi \ , \ p_{3,b} = \frac{j}{M}. \end{aligned} \tag{11}$$

3.1.4. FPPS (Full Pay per Shares). FPPS payment mechanism mining pools, also known as full PPS mining pools, are settled according to theoretical earnings after deducting mining fees for block rewards and miner fees.

The mining pool that chooses the FPPS payment mechanism for mining is defined as event V_4, and from Sections 3.1.2 and 3.1.3, it follows that the miner's mining revenue in event V_4 is

$$v_4 = \frac{1}{M} e_4 (1-\delta) KR. \tag{12}$$

The miner's gain from the miner's fee in event V_4 is

$$S_c\left(v_4\right) = \frac{1}{M} (1-\delta) K\varphi. \tag{13}$$

3.2. Mining Pool Selection Strategy under the Laplace Criterion. Laplace's criterion: Laplace's criterion, also known as the equal likelihood criterion, is based on the assumption that multiple states $C_j, j = \{1, 2, 3, \ldots, n\}$ of event $V_i, i = \{1, 2, 3, \ldots, m\}$ have the same probability $P(C_j)$ of occurring, i.e., $P(C_j) = (1/n), j = \{1, 2, 3, \ldots, n\}$, the total payoff of the event in each state is denoted as v_j^*, and then the expected payoff of the event is $E(V_i) = \sum_{i=1}^{n} P(C_j) * v_j^*$, $j = \{1, 2, \ldots, n\}$, where m refers to the number of possible events and N refers to the number of states in which the event may occur. The optimal choice of Laplace's criterion should satisfy $E_{V_i}^* = \max_{V_i = \{V_1, V_2, \ldots, V_m\}} E(V_i)$ in the expected revenue value of each event.

In Laplace's criterion, when the decision-maker cannot determine which event is easy to occur in the decision-making process, he has to think that the opportunity of various events is equal; that is, the probability of occurrence is equal. In other studies of mining pool selection strategies [16, 17], the variation of N in the PPLNS mechanism is used as the primary variable. This study did not focus on N change to highlight the effect of computing power allocation change on choosing four mine pool strategies. We believe that the change in N will only lead to two outcomes, and the probability of the two outcomes is equal: the partial proof of workload submitted by miners falls into the value range of N or not into the value range of N. This understanding is usually more in line with ordinary miners' knowledge of the various mining mechanisms when choosing a pool since not all miners are experts in understanding the mining pool. Our study controls for the results caused by changes in N. This control is more consistent with the requirements of Laplace decision-making, so it is reasonable to choose Laplace decision research in this paper.

Based on the Laplace criterion, the benefits of each of the four mining pool mechanisms can be summarized in conjunction with Section 3.1 as shown in Table 2.

Using the Laplace criterion principle, we assume that in a mining pool that includes a PPLNS payment mechanism, there are only two possibilities for partial workload proofs submitted by miners: falling into the range of values of N and not falling into the range of values of N. Under this criterion, the partial workload proofs submitted by miners in events V_2 and V_3 have the same probability of falling into both states a and b, i.e., $(M - j/M) = (j/M), N = (k-1)M + (1/2)M = (k-1/2)M, k \in [1, K]$. Let the expected revenue of the four mining pool mechanisms be $E(V_1), E(V_2), E(V_3)$, and $E(V_4)$. The following conclusions can be drawn from Table 2.

Table 2: Benefits of each of the four mining pool mechanisms under the Laplace criterion.

Payment mechanisms	Events V_i	Status C_j	Probability $P(C_j)$	Total revenue v_j^*
PPS	V_1	—	—	$v_1^* = (1/M)e_1(1-\delta)KR$
PPLNS	V_2	a	$M - j/M$	$v_{2,a}^* = (k-1/N)e_2(1-\delta)KR + (k-1/N)(1-\delta)K\varphi$
		b	j/M	$v_{2,b}^* = (k/N)e_2(1-\delta)KR + (k/N)(1-\delta)K\varphi$
PPS+	V_3	a	$M - j/M$	$v_{3,a}^* = (1/M)e_3(1-\delta)KR + (k-1/N)(1-\delta)K\varphi$
		b	j/M	$v_{3,b}^* = (1/M)e_3(1-\delta)KR + (k/N)(1-\delta)K\varphi$
FPPS	V_4	—	—	$v_4^* = (1/M)e_4(1-\delta)KR + (1/M)(1-\delta)K\varphi$

Table 3: Matrix of values for $R_E(i, j)$.

$R_E(i, j)$	$E(V_1)$	$E(V_2)$	$E(V_3)$	$E(V_4)$
$E(V)_1$	0	$((e_1 - e_2)R - \varphi/e_2R + \varphi)$	$((e_1 - e_3)R - \varphi/e_3R + \varphi)$	$((e_1 - e_4)R - \varphi/e_4R + \varphi)$
$E(V)_2$	$((e_2 - e_1)R + \varphi/e_1R)$	0	$((e_2 - e_3)R/e_3R + \varphi)$	$((e_2 - e_4)R/e_4R + \varphi)$
$E(V)_3$	$((e_3 - e_1)R + \varphi/e_1R)$	$((e_3 - e_2)R/e_2R + \varphi)$	0	$((e_3 - e_4)R/e_4R + \varphi)$
$E(V)_4$	$((e_4 - e_1)R + \varphi/e_1R)$	$((e_4 - e_2)R/e_2R + \varphi)$	$((e_4 - e_3)R/e_3R + \varphi)$	0

$$
\begin{aligned}
E(V_1) &= \frac{1}{M}e_1(1-\delta)KR,\\
E(V_2) &= \frac{1}{M}e_2(1-\delta)KR + \frac{1}{M}(1-\delta)K\varphi,\\
E(V_3) &= \frac{1}{M}e_3(1-\delta)KR + \frac{1}{M}(1-\delta)K\varphi,\\
E(V_4) &= \frac{1}{M}e_4(1-\delta)KR + \frac{1}{M}(1-\delta)K\varphi.
\end{aligned}
\tag{14}
$$

Let $R_E(i, j) = (E(V_i)/E(V_j)) - 1$ and obtain $R_E(i, j)$ taking matrix as shown in Table 3.

As can be seen from Table 3, for events V_1, when $e_1 - e_2 < (\varphi/R)$, $e_1 - e_3 < (\varphi/R)$, $e_1 - e_4 < (\varphi/R)$, and $e_1 < (3\varphi + R/4R)$, there is $E(V_1) < \min_{i=\{2,3,4\}} E(V_i)$, and the mining pool with the PPS payment mechanism is not selected at this time. When $e_1 - e_2 > (\varphi/R)$, $e_1 - e_3 > (\varphi/R)$, $e_1 - e_4 > (\varphi/R)$, and $e_1 > (3\varphi + R/4R)$, there is $E(V_1) > \max_{i=\{2,3,4\}} E(V_i)$, and the mining pool with the PPS payment mechanism is the optimal choice at this point.

For event V_2, when $e_1 - e_2 > (\varphi/R)$, $E(V_1) > E(V_2)$, and a mining pool with a PPLNS payment mechanism is not selected. When $e_1 - e_2 < (\varphi/R)$, $E(V)_1 < E(V_2)$, at which point if $e_2 - e_3 < 0$ or $e_2 - e_4 < 0$, there is $E(V_2) < \max_{i=\{3,4\}} E(V_i)$, the mining pool that does not select the PPLNS payment mechanism. If $e_2 - e_3 > 0$, $e_2 - e_4 > 0$, and $e_2 > (R - \varphi/4R)$, there is $E(V_2) > \max_{i=\{3,4\}} E(V_i)$ and at this point the mining pool with the PPLNS payment mechanism is optimal choice.

For event V_3, when $e_1 - e_3 > (\varphi/R)$ and $e_2 - e_3 > 0$, there is $E(V_3) < \max_{i=\{1,2\}} E(V_i)$, and the mining pool with PPS + payment mechanism is not selected. When $e_1 - e_3 < (\varphi/R)$ and $e_2 - e_3 < 0$, there is $E(V_3) > \max_{i=\{1,2\}} E(V_i)$, at which point if $e_3 - e_4 < 0$ and $e_3 < (R - \varphi/4R)$, there is $E(V)_3 < E(V_4)$, and the mining pool with the PPS + payment mechanism is not selected. If $e_3 - e_4 > 0$ and $e_3 > (R - \varphi/4R)$, there is $E(V_3) > \max_{i=\{1,2,4\}} E(V_i)$, and the mining pool with PPS + payment mechanism is the optimal choice.

For event V_4, when $e_1 - e_4 > (\varphi/R)$, $e_2 - e_4 > 0$, and $e_3 - e_4 > 0$, there is $E(V_4) < \min_{i=\{1,2,3\}} E(V_i)$, and the mining pool with FPPS payment mechanism is not selected. When $e_1 - e_4 < (\varphi/R)$, $e_2 - e_4 < 0$, $e_3 - e_4 < 0$, and $e_4 > (R - \varphi/4R)$, there is $E(V_4) > \max_{i=\{1,2,3\}} E(V_i)$, and at this point the mining pool with FPPS payment mechanism is the optimal choice.

In particular, when $e_1 - e_2 = (\varphi/R)$, $e_1 - e_3 = (\varphi/R)$, $e_1 - e_4 = (\varphi/R)$, $e_2 - e_3 = 0$, and $e_3 - e_4 = 0$, i.e., when $e_1 = (3\varphi + R/4R)$ and $e_2 = e_3 = e_4 = (R - \varphi/4R)$, all have $E(V_1) = E(V_2) = E(V_3) = E(V_4)$, and the choice of any payment mechanism mining pool is optimal.

4. Simulation and Analysis

This chapter evaluates the mining pool selection strategies under the Laplace criterion. We refer to the strategy that always selects one of the PPS, PPLNS, PPS+, and FPPS mining pools as strategy C_1, C_2, C_3, and C_4, and the strategy that uses the scheme proposed in this paper as strategy C_5. There are four events under strategy C_5, namely, V_1, V_2, V_3, and V_4, representing the selection of the PPS, PPLNS, and PPS + FPPS mining pools as the optimal choice for each case. In the discussion in Chapter 4, we analyzed the relationship between the mining pool selection strategy and the proportion of computing power allocation under the Laplace criterion. In this experiment, we will verify the effectiveness of the strategies proposed in this paper by comparing the total returns of each strategy under several different combinations of computing power allocation. To be able to verify more intuitively the validity of the strategies derived in this paper using the Laplace criterion, the following experiments were carried out.

4.1. Experimental Scenario. The experiments were implemented on a 64-bit Windows 10 system, with the Python 3 programming tool, using the NumPy scientific computing library for the simulations and the Matplotlib plotting library for the graphical presentation of the simulation results.

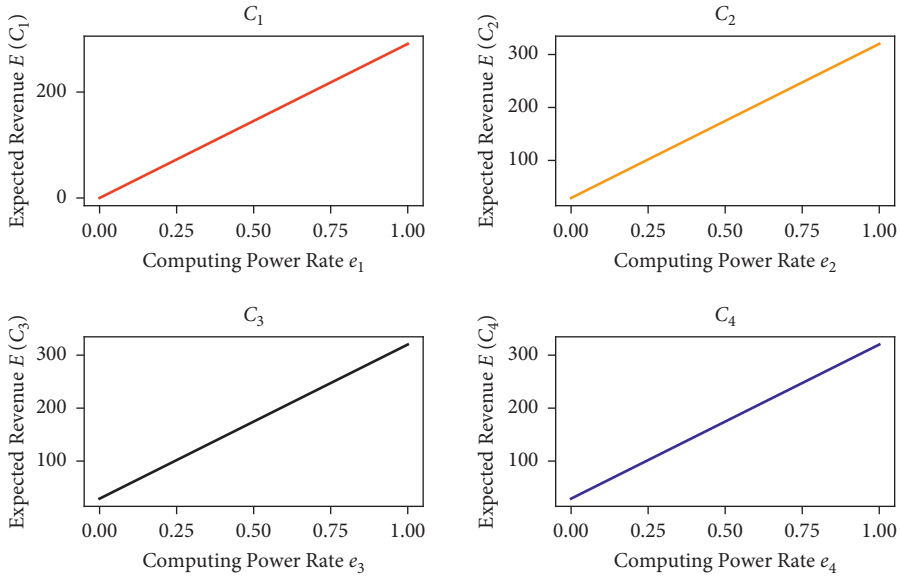

Figure 1: Expected revenue of strategy C_1, C_2, C_3, and C_4 under different computing power allocations.

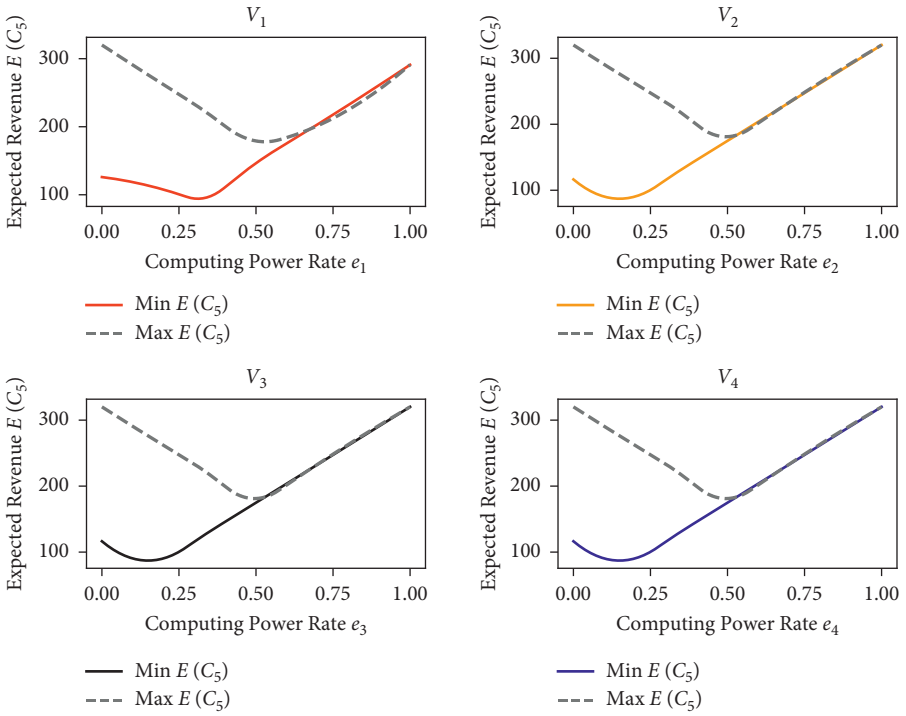

Figure 2: Expected revenue of strategy C_5 for each event under change in computing power.

4.2. Experiment Content. In this experiment, four mining pools are set up in the blockchain network, using the PPS, PPLNS, PPS+, and FPPS payment mechanisms, respectively, and each of them is governed by a computing power ratio of e_1, e_2, e_3, and e_4. All four pools will produce blocks in each round and receive block rewards and miner's fees corresponding to the computing power ratio, but the rewards are distributed according to their respective payment mechanisms, and each miner submits only partial proof of workload in each round. Assuming $M = 5$, $K = 15$, $\delta = 0.03$, $R = 100$, and $\varphi = 10$, the data with computing power e_1, e_2, e_3, and e_4 all in the range of [0, 1] and $e_1 + e_2 + e_3 + e_4 = 1$ are recorded as a combination, and the experiment gives the optimal mining pool selection strategy under a variety of different combinations of computing power taking values.

5. Results and Analysis

For strategies C_1, C_2, C_3, and C_4, experiments are conducted according to the possible values of their computing power e_1,

Table 4: Selected values for strategy C_5

	Percentage of computing power	0	0.225	0.325	0.475	0.675	1
e1	Min E (C5)	126.003	104.275	94.575	138.225	196.425	294
	Max E (C5)	320.1	254.625	225.525	181.875	196.425	291
e2	Min E (C5)	116.4	94.575	123.675	167.325	225.525	320.1
	Max E (C5)	320.1	254.625	225.525	181.875	225.525	320.1
e3	Min E (C5)	116.4	94.575	123.675	167.325	225.525	320.1
	Max E (C5)	320.1	254.625	225.525	181.875	225.525	320.1
e4	Min E (C5)	116.4	94.575	123.675	167.325	225.525	320.1
	Max E (C5)	320.1	254.625	225.525	181.875	225.525	320.1

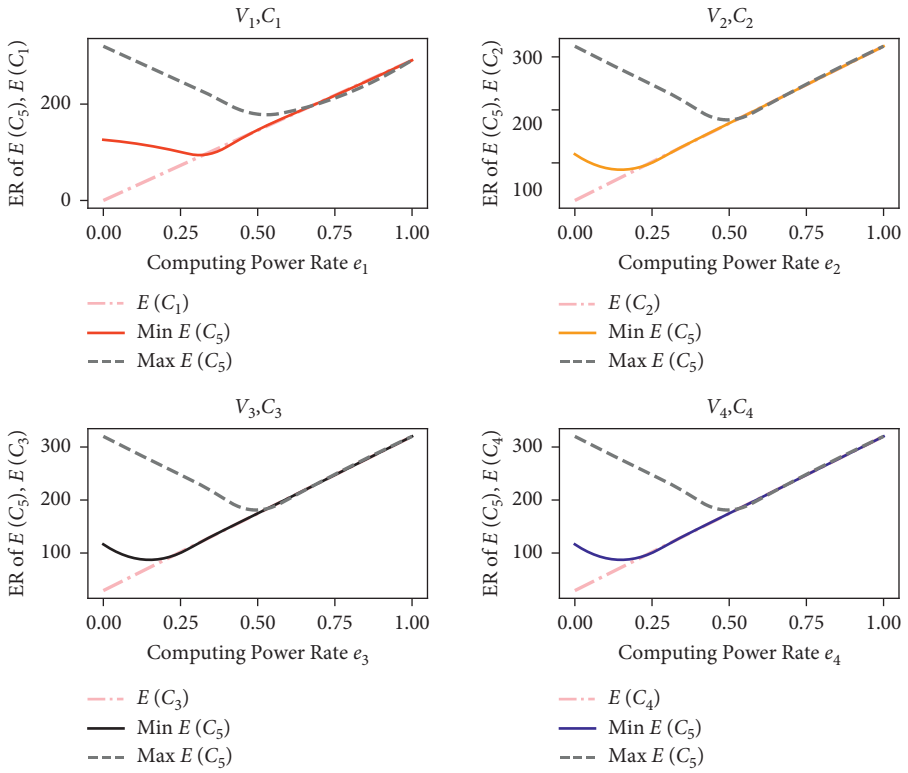

Figure 3: Expected revenue for strategy C_1, C_2, C_3, and C_4 versus strategy C_5 under different event choices.

e_2, e_3, and e_4, respectively. Figure 1 represents the expected revenue values of the strategy C_1, C_2, C_3, and C_4, when the computing power e_1, e_2, e_3, and e_4 takes values in the range [0, 1]. Figure 1 represents the relationship between the expected revenue $E(C_i)$ of the strategy C_i using a separate mine pool payment mechanism and the computing power e_i assigned to this strategy. As can be seen from Figure 1, the expected payoff of the C_1, C_2, and C_3, strategy is proportional to the computing power it is assigned to.

Figure 2 represents the expected revenue that can be fetched by strategy C_5 for each event computing power variation, and Table 4 shows the values taken for some of the points in strategy C_5. The dashed line represents the maximum expected revenue of strategy C_5 for each event computing power variation, and the realization represents the minimum expected revenue of strategy C_5 for each event computing power variation. In Figure 2, we show the relationship between the expected revenue of the strategy C_5 and the corresponding computing power e_i in each of the four events, V_1, V_2, V_3, and V_4, respectively. For any one event, the minimum expected gain is the greater of the gain of that event at computing power e and the gain of the other events that have equally divided the remaining computing power $(1 - e)$ other than the computing power of that event; the maximum expected gain arises when the other events have concentrated the remaining computing power $(1 - e)$ in one of the other events. Taking event V_1 as an example, the computing power of event V_1 is e_1, the gain is $E(V_1)$, and the gain of other events V_2 and V_3 is $E(V_2)$, $E(V_3)$, and $E(V_4)$. When $e_2 = e_3 = e_4 = (1 - e_1/3)$, there is $E(V_2) = E(V_3) = E(V_4)$ and $\text{Min}\, E(C_5) = \text{Min}\{E(V_1), E(V_i)\}$, $i = 2, 3, 4$; when $e_2 = 1 - e_1$, $e_3 = e_4 = 0$, there is $\text{Max}\, E(C_5) = \text{Max}\{E(V_1), E(V_2)\}$. When $E(V_1) = E(V_2) = E(V_3) = E(V_4)$, take the theoretical minimum, the solid line turning point in the diagram; when $E(V_1) = E(V_2)$, $\text{Max}\, E(C_5)$ coincides with the value of $\text{Min}\, E(C_5)$, both the

points in the diagram where the realized and dashed lines intersect.

As can be seen from Figure 2, the optimal choice of strategy events changes depending on the amount of computing power allocated to e_1, e_2, e_3, and e_4; when $e_1 = 0.325$, and $e_2 = e_3 = e_4 = 0.225$, i.e., when $e_1 = (3\varphi + R/4R)$ and $e_2 = e_3 = e_4 = (R - \varphi/4R)$, strategy C_5 takes the minimum expected revenue of $\text{Min}\, E(C_5) = E(V_1) = E(V_2) = E(V_3) = E(V_4)$, at which point the choice of any mechanism of the mining pool is optimal.

Figure 3 shows the expected revenue of strategy C_1, C_2, C_3, and C_4 compared to strategy C_5 under different event choices depending on the change in computing power, where the dotted line represents the expected revenue of strategy C_1, C_2, C_3, and C_4. In this chapter, the computing power of the four events of policy C_5 corresponds to that of strategies C_1, C_2, C_3, and C_4, respectively. In Figure 3, we group [event V_i, strategy C_i] and compare the relationship between the expected revenues of strategy C_5 and strategy C_i in each group, using the computing power e_i as the variable. Combined with Table 2, it can be seen that in event V_1, when $e_1 < (3\varphi + R/4R)$, strategy C_5 does not select a mining pool with a PPS payment mechanism, and when $e_1 > (3\varphi + R/4R)$, strategy C_5 will select a payment mechanism based on a ratio of e_1, e_2, e_3, and e_4, at which point the mining pool that selects a PPS payment mechanism will receive the minimum expected revenue $\text{Min}\, E(V_1)$, at which point the maximum expected revenue $\text{Max}\, E(V_1)$ is provided by a mining pool with another payment mechanism. Once the e_1 ratio of computing power grows to meet $\text{Min}\, E(V_1) = \text{Max}\, E(V_1)$, the mining pool with the PPS payment mechanism becomes the optimal choice. Similarly in events V_2, V_3, and V_4, when $e_2 < (R - \varphi/4R)$, strategy C_5 does not select the pool with the PPLNS payment mechanism, and when $e_2 > (R - \varphi/4R)$, the pool with the PPLNS payment mechanism will obtain the minimum expected revenue $\text{Min}\, E(V_2)$, and the pool with the PPLNS payment mechanism becomes the optimal choice after the proportion of computing power e_2 grows to satisfy $\text{Min}\, E(V_2) = \text{Max}\, E(V_2)$. When $e_3 < (R - \varphi/4R)$, strategy C_5 does not select the pool with the PPS + payment mechanism, and when $e_3 > (R - \varphi/4R)$, the pool with the PPS + payment mechanism will obtain the minimum expected revenue $\text{Min}\, E(V_3)$, and the pool with the PPS + payment mechanism becomes the optimal choice after the computing power e_3 grows proportionally to satisfy $\text{Min}\, E(V_3) = \text{Max}\, E(V_3)$. When $e_4 < (R - \varphi/4R)$, strategy C_5 does not select the pool with FPPS payment mechanism; when $e_4 > (R - \varphi/4R)$, the pool with FPPS payment mechanism will get the minimum expected revenue $\text{Min}\, E(V_4)$, and the pool with FPPS payment mechanism becomes the optimal choice after the proportion of computing power e_4 grows to satisfy $\text{Min}\, E(V_4) = \text{Max}\, E(V_4)$.

As can be seen from Figure 3, when the proportion of computing power represented by strategy C_1, C_2, C_3, and C_4 is high, the expected revenue obtained by strategy C_5 is equal to the expected revenue obtained by strategy C_1, C_2, C_3, and C_4; when the proportion of computing power represented by strategy C_1, C_2, C_3, and C_4 is low, the expected revenue obtained by strategy C_5 is higher than the expected revenue obtained by strategy C_1, C_2, C_3, and C_4. This indicates that strategy C_5 is superior to strategy C_1, C_2, C_3, and C_4.

6. Conclusion

This paper examines the problem of pool selection faced by miners when mining in blockchain networks. Consider the impact on the revenue of miners choosing a pool with a different payment mechanism when the four common pool payment mechanisms compete for blockchain network computing power. We adopt Laplace's criterion for the optimal selection strategy for four mining pools with different computing power and design corresponding experiments to evaluate the proposed pool selection strategy, and the experimental results verify the effectiveness of this pool selection strategy. This paper has shortcomings in the following questions:

RQ1: How to implement a selection strategy for multiple payment mechanism pools when miners submit multiple partial workload certificates in a single round.

RQ2: How to implement a selection strategy for multiple payment mechanism pools in the case of changing computing power allocation.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

No potential conflicts of interest were reported by the authors.

Acknowledgments

This work was supported by the National Natural Science Foundation of China, under Grant no. 61373162, and the Sichuan Provincial Science and Technology Department Project, under Grant no. 2022YFG0161.

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system [EB/OL]," 2008, https://bitcoin.org/bitcoin.pdf.

[2] Li Dong and W. Jinwu, "Theory, application fields and challenge of the blockchain technology[J]," *Telecommunications Science*, vol. 32, no. 12, pp. 20–25, 2016.

[3] A. Liu, X. Du, Na Wang, and S. Z Li, "Research progress of blockchain technology and its application in information security[J]," *Journal of Software*, vol. 29, no. 7, pp. 2092–2115, 2018.

[4] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Transactions on Services Computing*, vol. 11 page, 2022.

[5] J. Leng, G. Ruan, P. Jiang et al., "Blockchain-empowered sustainable manufacturing and product lifecycle management in Industry 4.0: a survey," *Renewable and Sustainable Energy Reviews*, vol. 132, Article ID 110112, 2020.

[6] J. Leng, S. Ye, M. Zhou et al., "Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 237–252, 2021.

[7] Y. Yuan and F. Wang, "Blockchain:the state of the art and future trends[J]," *Acta Automatica Sinica*, vol. 42, no. 04, pp. 481–494, 2016.

[8] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards secure and privacy-preserving data sharing for COVID-19 medical records: a blockchain-empowered approach," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 271–281, 2022.

[9] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities," *Computer Standards & Interfaces*, vol. 76, p. 103517, 2021.

[10] L. Tan, K. Yu, C. Yang, and A. K. Bashir, "A blockchain-based shamir's threshold cryptography for data protection in industrial internet of things of smart city," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (MobiCom 2021), Virtual Conference*, New Orleans, Louisiana, October 2021.

[11] J. Leng, P. Jiang, K. Xu et al., "Makerchain: a blockchain with chemical signature for self-organizing process in social manufacturing," *Journal of Cleaner Production*, vol. 234, pp. 767–778, 2019.

[12] J. Leng, D. Yan, Q. Liu et al., "ManuChain: combining permissioned blockchain with a holistic optimization model as Bi-level intelligence for smart manufacturing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 182–192, 2020.

[13] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77215–77226, 2020.

[14] L. Tan, H. Xiao, X. Shang, Y. Wang, F. Ding, and W. Li, "A blockchain-based trusted service mechanism for crowdsourcing system," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, in *Proceedings of the IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–6, Antwerp, Belgium, May 2020.

[15] C. Tang, C. Li, X. Yu, Z. Zheng, and Z. Chen, "Cooperative mining in blockchain networks with zero-determinant strategies," *IEEE Transactions on Cybernetics*, vol. 50, no. 10, pp. 4544–4549, 2020.

[16] Di Jian and W. Lin, "Research and analysis of mining pool selection strategy in blockchain[J]," *Computer Application Research*, vol. 37, no. 06, pp. 1804–1807, 2020.

[17] R. Qin, Y. Yuan, and F.-Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 748–757, Sept. 2018.

[18] M. Rosenfeld, "Analysis of Bitcoin pooled mining reward systems," 2011, https://arxiv.org/abs/1112.4980.

[19] M. Skorjanc, "How mining pools distribute rewards? PPS vs FPPS vs PPLNS [EB/OL]," 2019, https://www.nicehash.com/blog/post/how-mining-pools-distribute-rewards-pps-vs-fpps-vs-pplns.

[20] L. Tech, "Different bitcoin mining pool payment methods (PPS vs FPPS vs PPLNS vs PPS+) [EB/OL]," 2018, https://medium.com/luxor/mining-pool-payment-methods-pps-vs-pplns-ac699f44149f.

[21] T. MineBest, "Different mining pool payouts explained: PPS vs. FPPS vs. PPLNS vs. PPS+ [EB/OL]," 2021, https://minebest.com/blog/pps-vs-fpps-vs-pplns-vs-pps-mining-pool-payouts-explained.

[22] Dr Haribo, "Comparison of mining pools [EB/OL]," 2022, https://en.bitcoin.it/wiki/Comparison_of_mining_pools.

[23] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions, Financial Cryptography and Data Security," in *Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science*, J. Grossklags and B. Preneel, Eds., vol. 9603, pp. 477–498, Springer, Berlin, Heidelberg, 2017.

[24] Y. Zolotavkin, J. García, and C. Rudolph, "Incentive compatibility of Pay per last N Shares in bitcoin mining pools, Lecture Notes in Computer Science," in *Decision and Game Theory for Security. GameSec 2017. Lecture Notes in Computer Science*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds., vol. 10575, pp. 21–39, Springer, Cham, 2017.

[25] Y. Liu, X. Chen, L. Zhang, C. Tang, and H. Kang, "An intelligent strategy to gain profit for bitcoin mining pools," *2017 10th International Symposium on Computational Intelligence and Design (ISCID)*, in *Proceedings of the 2017 10th International Symposium on Computational Intelligence and Design (ISCID)*, pp. 427–430, Hangzhou, China, December 2017.

[26] R. Zhang and B. Preneel, "Publish or perish: a backward-compatible defense against selfish mining in bitcoin, Topics in Cryptology - CT-RSA 2017," in *Topics in Cryptology – CT-RSA 2017. CT-RSA 2017. Lecture Notes in Computer Science*, H. Handschuh, Ed., vol. 10159, pp. 277–292, Springer, Cham, 2017.

[27] I. Eyal, "The miner's dilemma," *2015 IEEE Symposium on Security and Privacy*, in *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, pp. 89–103, San Jose, CA, USA, May 2015.

[28] E. Altman, D. Menasché, A. Reiffers-Masson et al., "Blockchain competition between miners: a game theoretic perspective," *Frontiers in Blockchain*, vol. 2, p. 26, 2020.

[29] S. Singh, M. Salim, M. Cho, J. Cha, Y. Pan, and J. Park, "Smart contract-based pool hopping attack prevention for blockchain networks," *Symmetry*, vol. 11, no. 7, p. 941, 2019.

[30] T. Yang and Z. Xue, "The game problem and optimization among mining pools in blockchain systems[J]," *Communications Technology*, vol. 52, no. 05, pp. 1189–1195, 2019.

[31] L. Fan, H. Zheng, J. Huang, Z. Li, and Y. Jiang, "A cooperative evolutionary approach for blockchain mining pools based on adaptive zero determinant strategy," *Computer Applications*, vol. 39, no. 03, pp. 918–923, 2019.

[32] A. Kaci and A. Rachedi, "PoolCoin: toward a distributed trust model for miners' reputation management in blockchain," *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, in *Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, Las Vegas, NV, USA, January 2020.

[33] Y. Velner, J. Teutsch, and L. Luu, "Smart contracts make bitcoin mining pools vulnerable, Financial Cryptography and Data Security," in *Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science*, vol. 10323, pp. 298–316, Springer, Cham, 2017.

[34] Na Ruan, H. Liu, and S. Xueming, "The "catfish effect" among mining attackers in blockchain with proof-of-work consensus mechanism," *Journal of Computer Science*, vol. 44, no. 01, pp. 177–192, 2021.

[35] Y. Wang, C. Tang, F. Lin, Z. Zheng, and Z. Chen, "Pool strategies selection in PoW-based blockchain networks:

game-theoretic analysis," *IEEE Access*, vol. 7, pp. 8427–8436, 2019.

[36] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, 2018.

[37] C. Xu, K. Zhu, R. Wang, and Y. Xu, "Dynamic selection of mining pool with different reward sharing strategy in blockchain networks," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[38] Team F2pool, "Starting amounts and fees for each currency [EB/OL]," 2018, https://blog.f2pool.com/zh/faq/threshold.

[39] Team Viabtc, "Tariff rates[EB/OL]," 2019, https://www.viabtc.com/pricing.

[40] Team Antpool, "Miner configurations and rates [EB/OL]," 2022, https://antpoolhelp.zendesk.com/hc/zh-cn/articles/900001014643.

[41] Team BTC.com, "BTC.com pool's rates, settlement methods and starting amounts [EB/OL]," 2022, https://help.pool.btc.com/hc/zh-cn/articles/900001116943-BTC-com.