IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received May 10, 2020, accepted May 23, 2020, date of publication May 27, 2020, date of current version June 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2997996

Mining Pool Game Model and Nash Equilibrium Analysis for PoW-Based Blockchain Networks

WENBAI LI[1,2], (Member, IEEE), MENGWEN CAO[2], YUE WANG[2], CHANGBING TANG[3], (Member, IEEE), AND FEILONG LIN[2], (Member, IEEE)

[1]College of Economics and Management, Zhejiang Normal University, Jinhua 321004, China
[2]College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China
[3]College of Physics and Electronics Information Engineering, Zhejiang Normal University, Jinhua 321004, China

Corresponding author: Feilong Lin (bruce_lin@zjnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61877055, and in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY18F030013.

ABSTRACT Blockchain technology, has the characteristics of decentralization, openness and transparency, so that everyone can participate in database recording. Therefore, blockchain technology has a good application prospect in various industries. As the most successful application of blockchain technology, the Bitcoin system applies the Proof of Work (PoW) consensus mechanism. Under the PoW consensus mechanism, each miner competes through his own power to solve a SHA256 mathematical problem together, so as to gain profits. Due to the difficulty of the cryptography puzzle, miners tend to join the mining pool to obtain stable income. And the block withholding attacks will be carried out between the mining pools, so as to maximize his own income by controlling the infiltration rate dispatched to other mining pools. In this paper, we build a game model between mining pools based on the PoW consensus algorithm, and analyze its Nash equilibrium from two perspectives. The influence of the mining pools' power, the ratio of the power to be infiltrated, and the betrayed rate of dispatched miners on the mining pool's infiltration rate selection and income were explored, and the results were obtained through numerical simulations.

INDEX TERMS Blockchain, PoW consensus, game model, Nash equilibrium.

I. INTRODUCTION

Blockchain is a kind of chained data structure which combines data blocks in chronological order and ensures the tamper proof and forgery proof distributed ledger by cryptography. It uses a distributed consensus algorithm to generate and update data, uses cryptography to ensure the security of data transmission and access, uses the intelligent contract composed of automatic script code to program and operate data [1]. Because of its advantages in reducing costs, improving security and decentralization, blockchain technology has a wide range of application prospects, such as big data [2], smart grid [3], [4], Internet of Things [5], medical use [6]. Blockchain also has potentially huge application value in financial fields such as international exchange, letters of credit, equity registration, and stock exchanges. The application of blockchain technology in the financial industry can eliminate the need for third-party intermediary links and achieve direct peer-to-peer docking, thereby greatly reducing costs and quickly completing transaction payments [7]. Blockchain can also be naturally combined in the field of logistics. It facilitates to reduce logistics costs and improve the efficiency of supply chain management [8], [9].

The consensus mechanism is an important part of blockchain technology, which determines the degree of decentralization in blockchain technology, as well as the security and efficiency of blockchain technology. It allows the nodes on the entire network to reach a consensus and create a trust-free bookkeeping mechanism on the blockchain to ensure the consistency and authenticity of each transaction on all bookkeeping nodes. As the most successful application of blockchain technology, the Bitcoin system applies a Proof of Work (PoW) consensus mechanism. The core idea of the PoW consensus mechanism is to ensure the consistency of data and the security of consensus by introducing the computing power competition to the distributed nodes. In the system, each node competes with its own computing power to jointly solve a SHA256 mathematical problem, that is, to find a nonce in the entire network to ensure that the double SHA256 operation result of the block header

The associate editor coordinating the review of this manuscript and approving it for publication was Zhibo Wang.

of the current block is less than or equal to a predefined value. Once a node finds a random number that meets the requirements, the node will get the bookkeeping right of the current block as a reward, and the bookkeeper will also get a certain income [10], [11]. The above-mentioned process of obtaining rewards by implementing bookkeeping is also called ''mining'', and the nodes participating in mining are called ''miners'' [12]. Miners receive benefits based on their own computing power. It is difficult for small miners to succeed in mining alone.In order to obtain a more stable income, the miners choose to join the mining pool and mine together with other miners [13], and share rewards according to their own computing power [14].

A mining pool consists of a pool administrator and several miners. Miners use computing power to mine and send a partial Proofs of Work (PPoW) or a full Proofs of Work (FPoW) to obtain a gain proportional to the computing power. Sending part of the workload proof is not valuable to the Bitcoin system, and can only be used as a standard for measuring the miner's contribution to the computing power. In other words, the miner did not contribute effective computing power but obtained part of the profit of the mining pool. This behavior is called block withholding attacks. In a mining pool, miners can perform block withholding attacks on the mining pool and share the benefits of the mining pool with other miners. However, mining pools can also use miners to infiltrate into other mining pools and conduct block withholding attacks on other mining pools to obtain revenue in order to increase the total revenue of their own mining pools. For example, mining pool i sends a miner to infiltrate into mining pool j, and the miner sends partial proofs of work in mining pool j. That is, the miner did not mine effectively in mining pool j, but received the proceeds from mining pool j. And bring the income back to the original mining pool i, thereby increasing the income of the original mining pool i. This is a block withholding attack between mining pools. And, there will be a situation where miners who infiltrate into mining pool j will betray, that is, the miners faithfully mine in the mining pool j and do not bring the revenue back to the original mining pool i. In this case, for the original mining pool i, the revenue is lost. That is, for the original mining pool i, the behavior of the miners is betrayal. So, how to determine whether the mining pool is attacking or not and how to identify the betrayal miners? We plan to sign corresponding agreements when miners join the mining pool. The agreement stipulates that miners in the mining pool shall not enter other mining pools. And from the beginning to the end of a round of mining, no other miners are allowed to join the mining pool. Then in each mining process, the number of miners in the mining pool is fixed. Once the miners in the mining pool enter into other mining pools, it is regarded as an ''attack'', and the system will automatically give the mining pool punishment measures. If it appears at the beginning of mining, the miners in one mining pool enter other mining pools. And until the end of one round of mining, the miner did not return, that is, the number of miners in the two mining pools no longer changed, and this miner was regarded as a betrayal miner in the original pool. In order to make the content of the paper research more standardized and rigorous, the mining pools studied in the paper are considered as the closed mining pools.

At present, there are also some research results on the mining dilemma. Lewenberg Y *et al.* mapped the miner's choice of mining pool into a cooperative game model, and the miner increased his own income by changing the mining pool he chose to join [15]. Tang *et al.* start with the mining dilemma of pow consensus algorithm, analyze the existence conditions of Nash equilibrium of miner's strategy selection in the process of pow consensus, and optimize miner's strategy selection with zero determinant strategy [16]. Fan *et al.* combined with time-series difference enhancement algorithm and adaptive zero determinant strategy to deal with the problem of mutual attacks between mining pools [17]. Wang Tiantian *et al.* used the deep gradient learning strategy gradient algorithm to study the strategy choice of iterative prisoner's dilemma and deal with the Nash equilibrium problem of mining dilemma [18]. Eyal analyzes the existence of the mining dilemma, that is, the Nash equilibrium chooses the attack strategy for the mining pool, and the profit when the mining pool chooses to attack is not higher than the profit when it chooses not to attack [19]. Chang *et al.* analyzed UBA(uncle-block attack)'s incentive compatibility and identified and modelled the critical systems- and environmental-parameters which determine the attack's impacts [20]. However, considering the blockchain system's participation in the reward and punishment system and the mining pool's betrayal rate, no relevant research results have appeared. The main contributions of this paper are summarized as follows.

- The mining pool game model from the perspective of system rewards and punishments is established and its Nash equilibrium is analyzed. We get the relationship between the profit of the mining pool and the reward and punishment in the Nash equilibrium.
- The mining pool game model from the perspective of block withholding attacks between mining pools is established. That is, the infiltrate rate and betrayal rate of the mining pool are considered. And the Nash equilibrium and the value of infiltrate rate under the Nash equilibrium are analyzed.
- The influence of the mining pool's computing power, the ratio of the power to be infiltrated, and the betrayed rate of dispatched miners on the mining pool's infiltration rate selection and income are explored. The results were verified through numerical simulation.

The organizational structure of this paper is as follows: From the perspective of adding a reward and punishment system to the blockchain system, a multi-pool mining game model is established, and its pure strategy Nash equilibrium and mixed strategy Nash equilibrium are analyzed in Section II. From the perspective of block withholding attacks between mining pools, that is, considers the infiltrate rate and betrayal rate of the mining pool, analyzes the Nash equilibrium and the value of infiltrate rate under the Nash equilibrium in Section III. Through numerical simulation, section IV explores the influence of the mining pool's computing power, the ratio of the power to be infiltrated, and the betrayed rate of dispatched miners on the mining pool's infiltration rate selection and income. We summarizes and prospects our work in Section V.

II. GAME ANALYSIS OF MINING POOLS

A. MODEL DESCRIPTION

Assume that in a blockchain system based on the PoW consensus, M mining pools are formed by miners to obtain revenue through mining. Suppose the mining power vector is $p = (p_1, \ldots, p_i, \ldots, p_M)$, p_i is the mining power of the mining pool i, mining pool i will send the miners in its own pool to infiltrate other pools for block withholding attacks. Let the total power income in the system be R, and $R = 1$. In the case of attacking the mining pool, the mining pool that chooses not to attack will get an extra reward of $a(0 \leq a \leq 1)$ given by the system, and the mining pool that chooses to attack will get the penalty of $ka(k \geq 1)$, where k is the proportion of penalty to reward. $d_i(d_i \geq 0)$ is the average profit of the pool that chooses to attack, d_i' is the final average gain from other mining pools when the pool i chooses to attack. Set the number of non attacking mining pools other than mining pool i as m, $m \in \{1, 2, \ldots, M-1\}$.

(1) When $m = M-1$, pool i choose not to attack, and the mining pool i gains $p_i \cdot R = p_i$, $i \in \{1, 2, \ldots, M\}$.

(2) When $0 \leq m < M-1$, mining pool i chooses not to attack, set $d_i' \geq 0$, then the profit of mining pool i is $p_i + a - (M-m-1)d_i$, if mining pool i chooses to attack, and its profit is $p_i - ka + (M-1)d_i'$, that is:

$$u_i = \begin{cases} p_i + a - (M-m-1)d_i, & i \text{ chooses N strategy} \\ p_i - ka + (M-1)d_i', & i \text{ chooses A strategy} \end{cases} \tag{1}$$

(3) When all mining pools choose to attack each other, their returns meet $\Sigma_{i=1}^{M}(M-1)d_i' = 0$.

Let's take $M = 2$ as an example, because here we only analyze the relationship between the system reward a and the mining pool to reach the Nash equilibrium, so the profit of the mining pool in the model obtained through the infiltrating power is temporarily represented by d. The third part will analyze d in detail. Their benefits are as follows:

1) NO MINING POOL ATTACK

When both mining pools choose N(Not to attack), that is, neither miner is sent to infiltrate into the other mining pool, and the profit obtained by mining pool 1 is $p_1 \cdot 1 = p_1$, in the same way, the profit of mining pool 2 is p_2.

2) A MINING POOL ADOPTS THE A(ATTACK) STRATEGY

If mining pool 1 chooses not to attack, it will receive a reward of a. Although mining pool 2 that chooses the attack strategy will be punished by ka, it will share the profits in pool 1 by infiltrating miners, so pool 1 will lose the return of d, then the return expression of pool 1 is $p_1 + a - d$, and the return expression of pool 2 is $p_2 - ka + d$. Similarly, mining pool 1 chooses to attack, earns d by infiltrate miners into mining pool 2, and gets punishment ka. The mining pool 2 that chooses not to attack gets a reward of a, but will lose the profit of d, then the return expression of pool 1 is $p_1 - ka + d$, and the return expression of pool 2 is $p_2 + a - d$.

TABLE 1. The meaning of the symbols that appear in the paper.

symbol	meaning
M	The number of mining pools in the system
p_i	The mining power of the mining pool i
R	The total power income in the system
a	The extra reward given by the system
ka	The penalty given by the system
k	The proportion of penalty to reward
d_i	The average profit of the pools that choose to attack
d_i'	The average profit of the pool i that chooses to attack
m	The number of non attacking mining pools other than mining pool i
p_{M+1}	The computing power of miners who dig alone
a_{ij}	The infiltrate rate of mining pool i to mining pool j
$a_{ij} \cdot p_i$	The infiltration power of mining pool i to mining pool j
δ_i	The betrayal rate of the submerged power of the mining pool i
$\overline{R}$	The average power income of the mining pool i

TABLE 2. Payoff of pool.

	N	A
N	p_1, p_2	$p_1 + a - d, p_2 - ka + d$
A	$p_1 - ka + d, p_2 + a - d$	$p_1 - ka - d', p_2 - ka + d'$

3) TWO MINING POOL ATTACKS

When the mining pools choose to attack, the mining pools infiltrate the miners into the other mining pool and are punished ka. Suppose that the final mining pool 2 receives more revenue from mining pool 1 than mining pool 1, then mining pool 1 loses d', mining pool 2 gets d', and mining pool 1's income expression is $p_1 - ka - d'$, the mining pool 2's income expression is $p_2 - ka + d'$.

B. NASH EQUILIBRIUM ANALYSIS

1) PURE STRATEGY NASH EQUILIBRIUM

When $a < d' < d < ka$ and $a - d < d' - ka < d - ka$. When the mining pool 1 chooses not to attack, the mining pool 2 increases its own revenue by selecting the non-attack strategy; when the mining pool 1 selects the attack strategy, the mining pool 2 will not significantly reduce the revenue by selecting the attack. It can be obtained that the Nash equilibrium points of the mining pool 1 and the mining pool 2 are (N, N) and (A, A).

When $d > d' > ka$. When the mining pool 1 chooses not to attack, the mining pool 2 increases its own revenue by selecting the attack strategy; when the mining pool 1 selects the attack strategy, the mining pool 2 will increase its own income by selecting the attack, so the Nash equilibrium is (A, A).

When $d' < d < a$ and $a - d > 0, d' - ka < d - ka < 0$. When the mining pool 1 chooses not to attack, the mining pool 2 will not reduce its own revenue by selecting the non-attack strategy; when the mining pool 1 selects the attack strategy, the mining pool 2 chooses not to attack the strategy to increase its own revenue than the attack strategy. At this time, the Nash equilibrium point is (N, N).

It is analyzed that in the case of $a < d' < d < ka$ and $a-d < d'-ka < d-ka$, the Nash equilibrium is (N, N) and (A, A). If both mining pools choose to attack each other, then the income of the two mining pools will not be high when the cooperation is selected, and the system revenue will also decrease. In order to improve system revenue, we apply the ZD strategy to the mining pool game.

2) MIXED STRATEGY NASH EQUILIBRIUM

The mining pool game has a unique mixed Nash equilibrium point. Set the probability that mining pool 1 chooses not to attack is $x, (0 \leq x \leq 1)$, and the probability that mining pool 2 chooses not to attack is $y, (0 \leq y \leq 1)$, then the expected return of mining pool 1 choosing not to attack is:

$$p_1 + (1 - y)(a - d), \tag{2}$$

the expected return of mining pool 2 choosing not to attack is:

$$yd + p_1 - ka - (1 - y)d'. \tag{3}$$

Under the mixed strategy Nash equilibrium point, the expected return of the mining pool choosing different strategies is the same, namely:

$$p_1 + (1 - y)(a - d) = yd + p_1 - ka - (1 - y)d', \tag{4}$$

namely,

$$y = \frac{(k+1)a + d' - d}{a + d'}. \tag{5}$$

Similarly, for mining pool 2, the expected return from choosing not to attack is:

$$p_2 + (1 - x)(a - d), \tag{6}$$

the expected return on the chosen attack is:

$$xd + p_2 - ka + (1 - x)d'. \tag{7}$$

According to the mixed strategy Nash equilibrium point, the mining pool chooses different strategies with the same expected return, which is:

$$p_2 + (1 - x)(a - d) = xd + p_2 - ka + (1 - x)d', \tag{8}$$

namely,

$$x = \frac{(k+1)a - d' - d}{a - d'}. \tag{9}$$

According to the expressions of x, y, we can get the conditions under which the mixed Nash equilibrium exists:

$$|a - d| > |ka - d'| \text{or} |a - d'| > |ka - d|. \tag{10}$$

Theorem 1: In the mixed strategy, for the mining pool 1, when $d - kd' < 0$, the probability of the mining pool 1 choosing not to attack x is inversely proportional to the value of a. When $d - kd' > 0$, the probability that the mining pool 1 chooses not to attack x is proportional to the value of a. The probability that the mining pool 2 chooses not to attack y is always proportional to the value of a, that is, the greater the value of a, the greater the probability that mining pool 2 chooses not to attack, and the conditions under which the mixed strategy Nash equilibrium exists are:

$$|a - d| > |ka - d'| \text{or} |a - d'| > |ka - d|. \tag{11}$$

Remark 1: When both mining pools attack each other, when the income of mining pool 1 is $p_1 - ka + d'$ and the income of mining pool 2 is $p_2 - ka - d'$, the above conclusions about x, y are opposite.

Corollary 1: Under the mixed strategy Nash equilibrium point, when $0 < a < a_1$, the expected return of the mining pool 1 e_1 is proportional to a. When $a_1 < a < 1$, the expected return e_1 of mining pool 1 is inversely proportional to a, where $a_1 = \frac{\overline{d}}{k} - d', \overline{d} = \sqrt{k^2d'^2 + kdd' + k^2dd' + kd^2}$.

Proof: Substituting Eq.(5) into Eq.(2), the expected return of the mining pool 1 is:

$$\begin{aligned} e_1 &= p_1 + (1 - y)(a - d) \\ &= p_1 + [1 - \frac{(k+1)a + d' - d}{a + d'}](a - d) \\ &= \frac{-ka^2 + (p_1 + d + kd)a + p_1d' - d^2}{a + d'}. \end{aligned} \tag{12}$$

Derivating e_1:

$$e_1' = \frac{-ka^2 - 2kd'a + dd' + kdd' + d^2}{(a + d')^2}. \tag{13}$$

Because $(a + d')^2 > 0$ holds, let $-ka^2 - 2kd'a + dd' + kdd' + d^2 = 0$. After calculation, the axis of symmetry is $a = -d' < 0$, and there is a root greater than zero,

$$\begin{aligned} a_1 &= \frac{kd' - \sqrt{k^2d'^2 + kdd' + k^2dd' + kd^2}}{-k} \\ &< \frac{kd' - \sqrt{k^2d'^2 + k^2dd' + k^2dd' + k^2d^2}}{-k} \\ &= -[d' - (d + d')] \\ &= d < 1. \end{aligned} \tag{14}$$

Therefore, when $0 < a < a_1$, $e_1' > 0$, the expected return of the mining pool 1 e_1 is proportional to a. When $a_1 < a < 1$, the expected return e_1 of mining pool 1 is inversely proportional to a, where $a_1 = \frac{\widetilde{d}}{k} - d'$, $\widetilde{d} = \sqrt{k^2d'^2 + kdd' + k^2dd' + kd^2}$. ■

Corollary 2: Under the mixed strategy Nash equilibrium point,

(i) when $\frac{d}{d'} > 1 + k$ and $0 < a < a_2$, the expected return of the mining pool 2 e_2 is proportional to a. When $a_2 < a < 1$, the expected return of the mining pool 2 e_2 is inversely proportional to a, where $a_2 = \frac{\widetilde{d}}{k} + d'$, $\widetilde{d} = \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}$.

(ii) When $\frac{d}{d'} < 1 + k$, $d' < 0.5$ and $a_3 < a < a_4$, the expected return of the mining pool 2 e_2 is proportional to a. When $0 < a < a_3$ or $a_4 < a < 1$, the expected return of the mining pool 2 e_2 is inversely proportional to a, where $a_3 = \frac{-\widetilde{d}}{k} + d'$, $a_4 = \frac{\widetilde{d}}{k} + d'$, $\widetilde{d} = \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}$.

Proof: Substituting Eq.(9) into Eq.(6), the expected return of the mining pool 2 is:

$$\begin{aligned} e_2 &= p_2 + (1 - x)(a - d) \\ &= p_2 + [1 - \frac{(k+1)a - d' - d}{a - d'}](a - d) \\ &= \frac{-ka^2 + (p_2 + d + kd)a - p_2d' - d^2}{a - d'}. \end{aligned} \tag{15}$$

Derivating e_2:

$$e_2' = \frac{-ka^2 + 2kd'a - dd' - kdd' + d^2}{(a - d')^2}. \tag{16}$$

Because $(a - d')^2 > 0$ is constant, let $-ka^2 + 2kd'a - dd' - kdd' + d^2 = 0$, after calculation, the axis of symmetry is $a = d' > 0$.

(1) When $\frac{d}{d'} > 1 + k$, $-ka^2 + 2kd'a - dd' - kdd' + d^2 = 0$ has a positive root:

$$\begin{aligned} a_2 &= \frac{kd' + \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}}{k} \\ &< \frac{kd' + \sqrt{k^2d'^2 - k^2dd' - k^2dd' + k^2d^2}}{k} \\ &= d' + (d - d') \\ &= d < 1. \end{aligned} \tag{17}$$

Therefore, when $0 < a < a_2$, $e_2' > 0$, the expected return of the mining pool 2 e_2 is proportional to a. When $a_2 < a < 1$, $e_2' < 0$, the expected return of the mining pool 2 e_2 is inversely proportional to a, where $a_2 = \frac{\widetilde{d}}{k} + d'$, $\widetilde{d} = \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}$. That's ($i$).

(2) When $\frac{d}{d'} < 1 + k$, for $-ka^2 + 2kd'a - dd' - kdd' + d^2 = 0$,

$$\begin{aligned} \Delta &= (2kd')^2 + 4k(d^2 - dd' - kdd') \\ &> 4(k^2d'^2 + d^2 - dd' - kdd') \\ &= 4[(kd' - d)^2 + kdd' - dd'] \\ &> 0. \end{aligned} \tag{18}$$

That is, the equation $-ka^2 + 2kd'a - dd' - kdd' + d^2 = 0$ always has two solutions a_3, a_4, $(0 < a_3 < a_4)$, and,

$$a_4 = \frac{kd' + \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}}{k} < \frac{2kd'}{k} = 2d'. \tag{19}$$

Therefore, when $d' < 0.5$ and $a_3 < a < a_4$, $e_2' > 0$, the expected return of the mining pool 2 e_2 is proportional to a. When $0 < a < a_3$ or $a_4 < a < 1$, $e_2' < 0$, the expected return of the mining pool 2 e_2 is inversely proportional to a, where $a_3 = \frac{-\widetilde{d}}{k} + d'$, $a_4 = \frac{\widetilde{d}}{k} + d'$, $\widetilde{d} = \sqrt{k^2d'^2 - kdd' - k^2dd' + kd^2}$. That is ($ii$). ■

III. ANALYSIS OF MINING POOL GAME MODEL ON INFILTRATE RATE AND BETRAYAL RATE

A. MODEL INTRODUCTION

This section will analyze the "d" in the previous model in detail. Suppose there are M mining pools in the system, and the initial computing power of the mining pool i is p_i. Assume that there are also miners who dig alone without adding the mining pool in the system, and consider all the separately miners as a whole, with a computing power of p_{M+1}, and satisfying $\Sigma_{i=1}^{M+1} p_i = 1$, then the total system revenue is also 1. $a_{ij} (i, j = 1, 2, \ldots, M, \Sigma_{j=1}^{M} a_{ij} = 1, 0 \leq a_{ij} < 1, 0 < a_{ii} \leq 1)$ is the infiltrate rate of mining pool i to mining pool j, $a_{ij} \cdot p_i$ represents the infiltration mining power of mining pool i to mining pool j, and a_{ii} is the computing power ratio reserved by the mining pool i itself. Among them, when the mining pool infiltrates miners into other mining pools, although some miners bring the profits obtained by infiltrating into the mining pool back to the original mining pool, some of them will also provide FPoW in the submerged pool to obtain the income but not bring back. That is to say, due to the betrayal of the miners, the power of the original mining pool decreases, while the effective power of the submerged mining pool increases. Let $\delta_i (0 \leq \delta_i < 1)$ be the betrayal rate of the submerged power of the mining pool i.

In the mining process, the computing power of the mining pool i can be divided into two parts: effective mining power and attack power. Then the income of the mining pool i is the income obtained by effective mining power and the income obtained by infiltrating into other mining pools through attack. The average power income of the mining pool is defined as follows.

Definition 1 (Average Power Income): Let the average power income of the mining pool i be the ratio of the total profit of the mining pool to the total power of the mining pool, and record it as $\bar{R}$.

Then the average power income of the mining pool i at step t is $\bar{R}_i(t)$:

$$\bar{R}_i(t) = \frac{r_i + \sum_{j=1, j\neq i}^{M} a_{ij} p_i (1 - \delta_i) \bar{R}_j(t-1) + c_i}{(1 - \sum_{j=1, j\neq i}^{M} a_{ij}\delta_i) p_i + \sum_{j=1, j\neq i}^{M} a_{ji} p_j}, \tag{20}$$

where,

$$r_i = \frac{a_{ii}p_i + \sum\limits_{j=1,j\neq i}^{M} a_{ji}\delta_j p_j}{\sum\limits_{j=1}^{M+1} a_{jj}p_j + \sum\limits_{j=1,j\neq i}^{M} a_{ji}\delta_j p_j + \sum\limits_{i=1,i\neq j}^{M} a_{ij}\delta_i p_i}, \tag{21}$$

$$c_i = \begin{cases} a, & i \text{ chooses N strategy,} \\ -ka, & i \text{ chooses A strategy.} \end{cases} \tag{22}$$

r_i is the profit obtained from the system by the mining pool's effective mining power.

That is, the ratio of the computing power $a_{ii}p_i$ retained by the mining pool i and the power of betrayed miners infiltrated from pool j but faithfully mine in pool i and the total effective computing power in the system. $\sum\limits_{j=1,j\neq i}^{M} a_{ij}p_i(1-\delta_i)\bar{R}_j(t-1)$ is the profit from the loyal miners (i.e. unbetrayed miners) sent for the mining pool i who infiltrate into the pool j. The total computing power of the mining pool i is $(1 - \sum\limits_{j=1,j\neq i}^{M} a_{ij}\delta_i)p_i + \sum\limits_{j=1,j\neq i}^{M} a_{ji}p_j$. That is, the loyal computing power of the mining pool i and the computing power of other mining pools infiltrating into the mining pool i. Let $A_i = \frac{\sum\limits_{j=1,j\neq i}^{M} a_{ji}p_j}{p_i}$ be the ratio of the power to be infiltrated of mining pool i. When there is no mining pool to choose to attack, the profit of mining pool i is $\frac{p_i}{\sum\limits_{j=1}^{M+1} p_j}$.

Theorem 2: When there are enough iterations in the game, the final return of the pool tends to be stable.

Proof: Set the average power income at the t step game of the mining pool is:

$$\bar{\mathbf{R}}(t) = (\bar{R}_1(t), \bar{R}_2(t), \ldots, \bar{R}_M(t))^T. \tag{23}$$

In each round, the profit obtained from the system by the effective mining power in the mining pool i is equally distributed to the actual total computing power of the mining pool i that includes the computing power infiltrate from other mining pools. Let $\mathbf{P}$ and $\mathbf{C}$ be as shown in formula (44) and (45) as shown at the bottom of the next page.

Where,

$$r_i = \frac{a_{ii}p_i + \sum\limits_{j=1,j\neq i}^{M} a_{ji}\delta_j p_j}{\sum\limits_{j=1}^{M+1} a_{jj}p_j + \sum\limits_{j=1,j\neq i}^{M} a_{ji}\delta_j p_j + \sum\limits_{i=1,i\neq j}^{M} a_{ij}\delta_i p_i}, \tag{24}$$

$$c_i = \begin{cases} a, & i \text{ chooses N strategy,} \\ -ka, & i \text{ chooses A strategy.} \end{cases} \tag{25}$$

Define a $M \times M$ matrix on infiltrate rate and betrayal rate:

$$\mathbf{H} = [\frac{a_{ij}p_i(1-\delta_i)}{(1 - \sum\limits_{k=1,k\neq i}^{M} a_{ik}\delta_i)p_i + \sum\limits_{k=1,k\neq i}^{M} a_{ki}p_k}]_{ij}. \tag{26}$$

When $i = j$, $H_{ij} = 0$. Because the power of mining pool i has infiltrated into the mining pool j in the t step, share the profit at the end of the $t - 1$ step game in the mining pool j. Then:

$$\bar{\mathbf{R}}(t) = \mathbf{P} + \mathbf{H} \cdot \bar{\mathbf{R}}(t-1) + \mathbf{C}. \tag{27}$$

Because the sum of each row of matrix $\mathbf{H}$ is less than 1, when t tends to infinity, there is:

$$\begin{aligned} \bar{\mathbf{R}}(t) &= \mathbf{P} + \mathbf{H} \cdot \bar{\mathbf{R}}(t-1) + \mathbf{C} \\ &= \sum_{t'=0}^{t-1} \mathbf{H}^{t'}(\mathbf{P}) + \sum_{t'=0}^{t-1} \mathbf{H}^{t'}(\mathbf{C}) + \mathbf{H}^{t}\bar{\mathbf{R}}(0) \\ &= \sum_{t'=0}^{t-1} \mathbf{H}^{t'}(\mathbf{P} + \mathbf{C}) + \mathbf{H}^{t}\bar{\mathbf{R}}(0) \\ &\xrightarrow{t\to\infty} (\mathbf{1} - \mathbf{H})^{-1}(\mathbf{P} + \mathbf{C}) \end{aligned} \tag{28}$$

The return of the mining pool i at step t is:

$$u_i(t) = [(1 - \sum_{j=1,j\neq i}^{M} a_{ij}\delta_i)p_i + \sum_{j=1,j\neq i}^{M} a_{ji}p_j] \cdot \bar{R}_i(t). \tag{29}$$

Then when the number of iterations of the game is enough, the final return of the mining pool is stable. ■

B. NASH EQUILIBRIUM ANALYSIS

The following takes $M = 2$ as an example to discuss the Nash equilibrium of the mining pool under various strategic options.

1) NO MINING POOL ATTACK

When both mining pools choose N (Not to attack), that is, $a_{ij} = a_{ji} = 0 (i, j = 1, 2)$, and the profit obtained by mining pool 1 is $p_1 \cdot 1 = p_1$, in the same way, the profit of mining pool 2 is p_2.

2) A MINING POOL ADOPTS THE *A*(ATTACK) STRATEGY

When mining pool 1 chooses not to attack and mining pool 2 chooses to attack. That is $a_{12} = 0$, $a_{21} > 0$, $\delta_2 \geq 0$. $a_{21}p_2\delta_2$ is the betrayal power of mining pool 2. p_3 is the total power of the individual mining in the system. Obviously $a_{33} = 1$. The effective mining power profit of mining pool 1 is:

$$r_1 = \frac{p_1 + a_{21}\delta_2 p_2}{p_1 + a_{22}p_2 + p_3 + a_{21}\delta_2 p_2}. \tag{30}$$

The average power income of mining pool 1 is the effective mining power income plus the reward obtained from the system when mining pool 1 chooses not to attack is divided equally by the mining computing power of mining pool 1 and mining pool 2. The average power income of mining pool 1 is:

$$\bar{R}_1 = \frac{r_1 + a}{p_1 + a_{21}p_2}. \tag{31}$$

The effective mining power profit of mining pool 2 is:

$$r_2 = \frac{a_{22}p_2}{p_1 + a_{22}p_2 + p_3 + a_{21}\delta_2 p_2}. \tag{32}$$

The average power income of mining pool 2 is the effective mining power income plus the income from the potential power without betrayal minus the punishment for choosing to attack mining pool 1, which is equally divided in the power without betrayal of mining pool 2. The average power income of mining pool 2 is:

$$\overline{R}_2 = \frac{r_2 + a_{21}p_2(1-\delta_2)\overline{R}_1 - ka}{(1-a_{21}\delta_2)p_2}. \tag{33}$$

Mining pool 2 will maximize its own income by controlling the infiltration rate to mining pool 1, that is, the value of $a_{21}(0 < a_{21} < 1)$. Because mining pool 1 does not respond to the attack of mining pool 2, the value of a_{21} when the mining pool 2 maximizes the return value is the stable state of the system. Thereby:

$$argmax_{a_{21}}\overline{R}_2(a_{21}) = a'_{21}. \tag{34}$$

Substitute the stable value a'_{21} to get the profit value of mining pool 1 and mining pool 2.

Similarly, when mining pool 2 chooses not to attack and mining pool 1 chooses to attack. That is $a_{12} > 0, \delta_1 \geq 0, a_{21} = 0$, $a_{12}p_1\delta_1$ is the betrayal power of mining pool 1. p_3 is the total power of the individual mining in the system. The effective mining power profit of mining pool 1 is:

$$r_1 = \frac{a_{11}p_1}{a_{11}p_1 + p_2 + p_3 + a_{12}\delta_1 p_1}. \tag{35}$$

The average power income of mining pool 1 is the effective mining power income plus the income from the potential power without betrayal minus the punishment for choosing to attack mining pool 2, which is equally divided in the power without betrayal of mining pool 1. The average power income of mining pool 1 is:

$$\overline{R}_1 = \frac{r_1 + a_{12}p_1(1-\delta_1)\overline{R}_2 - ka}{(1-a_{12}\delta_1)p_1}. \tag{36}$$

The effective mining power profit of mining pool 2 is:

$$r_2 = \frac{p_2 + a_{12}\delta_1 p_1}{a_{11}p_1 + p_2 + p_3 + a_{12}\delta_1 p_1}. \tag{37}$$

The average power income of mining pool 2 is the effective mining power income plus the reward obtained from the system when mining pool 2 chooses not to attack is divided equally by the mining computing power of mining pool 1 and mining pool 2. The average power income of mining pool 2 is:

$$\overline{R}_2 = \frac{r_2 + a}{p_2 + a_{12}p_1}. \tag{38}$$

Similarly, Mining pool 1 will maximize its own income by controlling the infiltration rate to mining pool 2, that is, the value of $a_{12}(0 < a_{12} < 1)$. Because mining pool 2 does not respond to the attack of mining pool 1, the value of a_{12} when the mining pool 1 maximizes the return value is the stable state of the system. Thereby:

$$argmax_{a_{12}}\overline{R}_1(a_{12}) = a'_{12}. \tag{39}$$

Substitute the stable value a'_{12} to get the profit value of mining pool 1 and mining pool 2.

3) TWO MINING POOL ATTACKS

When both mining pool 1 and mining pool 2 choose to attack, that is, $a_{12} > 0, \delta_1 \geq 0, a_{21} > 0, \delta_2 \geq 0$.

The effective mining power profit of mining pool 1 is:

$$r_1 = \frac{a_{11}p_1 + a_{21}\delta_2 p_2}{a_{11}p_1 + a_{22}p_2 + p_3 + a_{12}\delta_1 p_1 + a_{21}\delta_2 p_2}. \tag{40}$$

The average power income of mining pool 1 is the effective mining power income plus the income from the potential power without betrayal minus the punishment for choosing to attack mining pool 2, which is equally divided in the actual total power of mining pool 1 and the power infiltrated from mining pool 2. In stable state, the average power income of mining pool 1 is:

$$\overline{R}_1 = \frac{r_1 + a_{12}p_1(1-\delta_1)\overline{R}_2 - ka}{(1-a_{12}\delta_1)p_1 + a_{21}p_2}. \tag{41}$$

Similarly, the effective mining power profits of mining pool 2 is:

$$r_2 = \frac{a_{22}p_2 + a_{12}\delta_1 p_1}{a_{11}p_1 + a_{22}p_2 + p_3 + a_{12}\delta_1 p_1 + a_{21}\delta_2 p_2}. \tag{42}$$

$$\mathbf{P} = \left(\frac{r_1}{(1-\sum\limits_{j=2}^{M} a_{1j}\delta_1)p_1 + \sum\limits_{j=2}^{M} a_{j1}p_j}, \frac{r_2}{(1-\sum\limits_{j=1,j\neq 2}^{M} a_{2j}\delta_2)p_2 + \sum\limits_{j=1,j\neq 2}^{M} a_{j2}p_j}, \ldots, \frac{r_M}{(1-\sum\limits_{j=1}^{M-1} a_{Mj}\delta_M)p_M + \sum\limits_{j=1}^{M-1} a_{jM}p_j}\right)^T \tag{44}$$

$$\mathbf{C} = \left(\frac{c_1}{(1-\sum\limits_{j=2}^{M} a_{1j}\delta_1)p_1 + \sum\limits_{j=2}^{M} a_{j1}p_j}, \frac{c_2}{(1-\sum\limits_{j=1,j\neq 2}^{M} a_{2j}\delta_2)p_2 + \sum\limits_{j=1,j\neq 2}^{M} a_{j2}p_j}, \ldots, \frac{c_3}{(1-\sum\limits_{j=1}^{M-1} a_{Mj}\delta_M)p_M + \sum\limits_{j=1}^{M-1} a_{jM}p_j}\right)^T \tag{45}$$

$$\overline{R}_1(a_{12}, a_{21}) = \frac{r_1p_2 + (r_1+r_2)a_{12}p_1 - r_2a_{12}p_1\delta_1 - r_1a_{21}p_2\delta_2}{p_1p_2 + a_{12}p_1^2 + a_{21}p_2^2 - \delta_1a_{12}^2p_1^2 - \delta_2a_{21}^2p_2^2 + [(\delta_2 + \delta 1)a_{12}a_{21} - \delta_1a_{12} - \delta_2a_{21}]p_1p_2} \tag{46}$$

$$\overline{R}_2(a_{12}, a_{21}) = \frac{r_2p_1 + (r_1+r_2)a_{21}p_2 - r_1a_{21}p_2\delta_2 - r_2a_{12}p_1\delta_1}{p_1p_2 + a_{12}p_1^2 + a_{21}p_2^2 - \delta_1a_{12}^2p_1^2 - \delta_2a_{21}^2p_2^2 + [(\delta_2 + \delta 1)a_{12}a_{21} - \delta_1a_{12} - \delta_2a_{21}]p_1p_2} \tag{47}$$

The average power income of mining pool 2 is the effective mining power income plus the income from the potential power without betrayal minus the punishment for choosing to attack mining pool 1, which is equally divided in the actual total power of mining pool 2 and the power infiltrated from mining pool 1. In stable state, the average power income of mining pool 2 is:

$$\overline{R}_2 = \frac{r_2 + a_{21}p_2(1-\delta_2)\overline{R}_1 - ka}{(1-a_{21}\delta_2)p_2 + a_{12}p_1}. \tag{43}$$

In order to solve the values of $\overline{R}_1$ and $\overline{R}_2$ in the stable state, the simultaneous expression of (41)(43) can be used to obtain the expression of average power income related to a_{12} and a_{21} (see formula (46) and (47) as shown at the bottom of the previous page).

In each round of game, the mining pool will optimize its own revenue by controlling its own infiltration rate. When both mining pool 1 and mining pool 2 will not change their infiltration rate to increase revenue, this stable state will reach the Nash equilibrium. That is, for any pair of a'_{12} and a'_{21}, there are:

$$\begin{cases} argmax_{a_{12}}\overline{R}_1(a_{12}, a'_{21}) = a'_{12}; \\ argmax_{a_{21}}\overline{R}_2(a'_{12}, a_{21}) = a'_{21}. \end{cases} \tag{48}$$

For function $\overline{R}_i$, there are $\frac{\partial^2 \overline{R}_i}{\partial^2 \; a_i} < 0$. Therefore, in the Nash equilibrium state, the values of a_{12} and a_{21} satisfy:

$$\begin{cases} \dfrac{\partial \overline{R}_1(a_{12}, a_{21})}{\partial a_{12}} = 0; \\ \dfrac{\partial \overline{R}_2(a_{12}, a_{21})}{\partial a_{21}} = 0. \end{cases} \tag{49}$$

Corollary 3: When $\delta_1 = \delta_2 = 0$, that is, the miners sent by the mining pool to infiltrate into the other mining pools are loyal miners. The average power income of the two pools are:

$$\overline{R}_1(a_{12}, a_{21}) = \frac{r_1p_2 + (r_1 + r_2)a_{12}p_1}{p_1p_2 + a_{12}p_1^2 + a_{21}p_2^2}, \tag{50}$$

$$\overline{R}_2(a_{12}, a_{21}) = \frac{r_2p_1 + (r_1 + r_2)a_{21}p_2}{p_1p_2 + a_{12}p_1^2 + a_{21}p_2^2}. \tag{51}$$

Similarly, in each round of game, the mining pool will optimize its own revenue by controlling its own infiltration rate. When both mining pool 1 and mining pool 2 will not change their infiltration rate to increase revenue, this stable state will reach the Nash equilibrium. That is, for any pair of a'_{12} and a'_{21}, there are:

$$\begin{cases} argmax_{a_{12}}\overline{R}_1(a_{12}, a'_{21}) = a'_{12}; \\ argmax_{a_{21}}\overline{R}_2(a'_{12}, a_{21}) = a'_{21}. \end{cases} \tag{52}$$

Therefore, in the Nash equilibrium state, the values of a_{12} and a_{21} satisfy:

$$\begin{cases} \dfrac{\partial \overline{R}_1(a_{12}, a_{21})}{\partial a_{12}} = 0; \\ \dfrac{\partial \overline{R}_2(a_{12}, a_{21})}{\partial a_{21}} = 0. \end{cases} \tag{53}$$

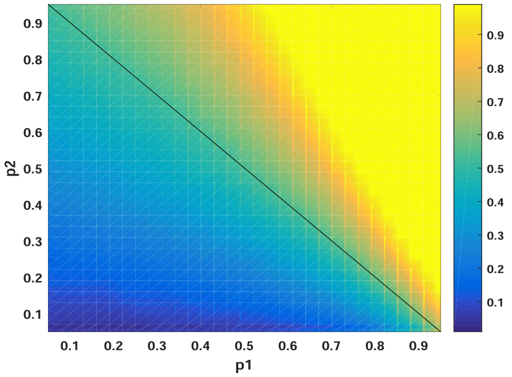

FIGURE 1. When $\delta_1 = 0.2$, the value of the infiltrate rate a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

IV. SIMULATION

Through numerical simulation, this section explores the influence of the mining pool's computing power, the ratio of the power to be infiltrated, and the betrayed rate of dispatched miners on the mining pool's infiltration rate selection and income.

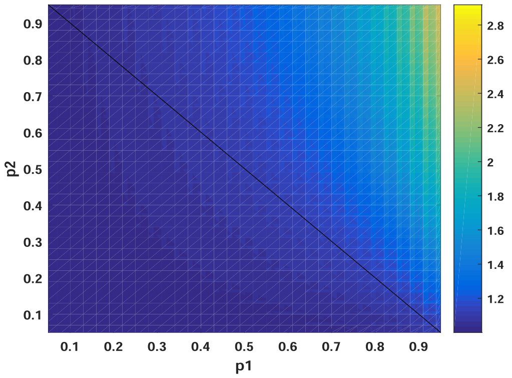

FIGURE 2. When $\delta_1 = 0.2$, the average power incomes of pool 1 in the case of the optimum infiltration.

We first consider the situation of one mining pool attack, assuming that mining pool 1 chooses the attack strategy and mining pool 2 chooses not to attack. In Fig.2-4, the betrayal rate of the miners dispatched by mining pool 1 is set to $\delta_1 = 0.2$, while Fig.5-7 and Fig.8-10 are $\delta_1 = 0.5$ and $\delta_1 = 0.8$. These figures show the value of the infiltrate rate a_{12} at the Nash equilibrium in the case of different p_1 and p_2, and the average power incomes of pool 1 and pool 2 in the case of the optimum infiltration. The horizontal and vertical coordinates in the figure represent the computing power of mining pool 1 p_1 and the computing power of mining pool 2 p_2, and different colors in the figure represent different target values.

By comparing the three sets of figures in Fig.2-10, we find that all have similar changes. Fig.2, Fig.5 and Fig.8 are the changes of the values of the infiltrate rate a_{12} at the Nash equilibrium in the case of different p_1 and p_2. It is found through observation that when the computing power of mining pool 2 gradually decreases, the infiltrate rate a_{12} of mining pool 1 also gradually decreases. When the total mining power of

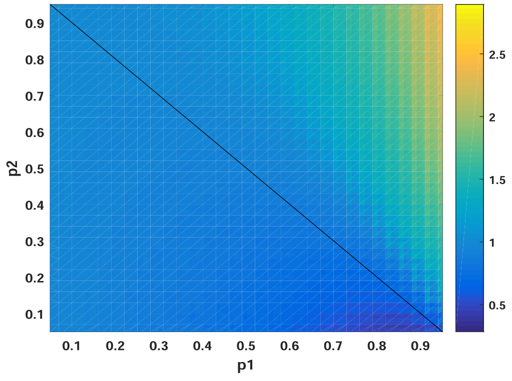

FIGURE 3. When $\delta_1 = 0.2$, the average power incomes of pool 2 in the case of the optimum infiltration.

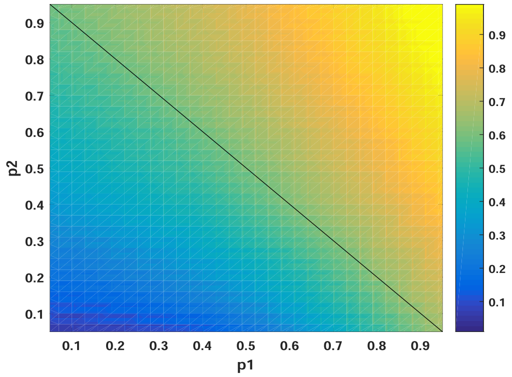

FIGURE 4. When $\delta_1 = 0.5$, the value of the infiltrate rate a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

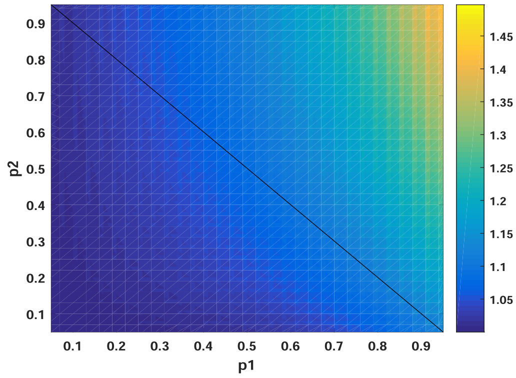

FIGURE 5. When $\delta_1 = 0.5$, the average power incomes of pool 1 in the case of the optimum infiltration.

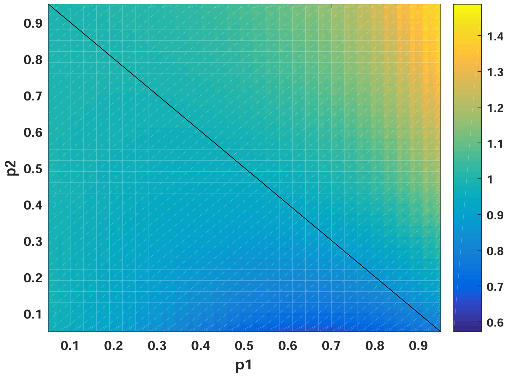

FIGURE 6. When $\delta_1 = 0.5$, the average power incomes of pool 2 in the case of the optimum infiltration.

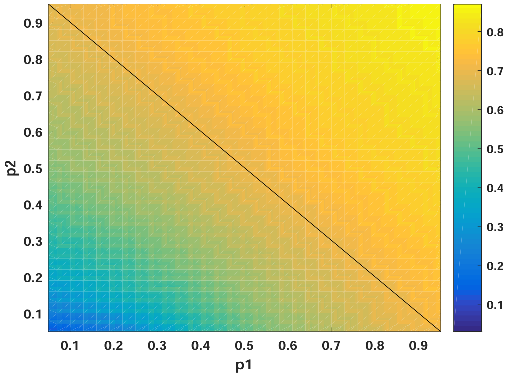

FIGURE 7. When $\delta_1 = 0.8$, the value of the infiltrate rate a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

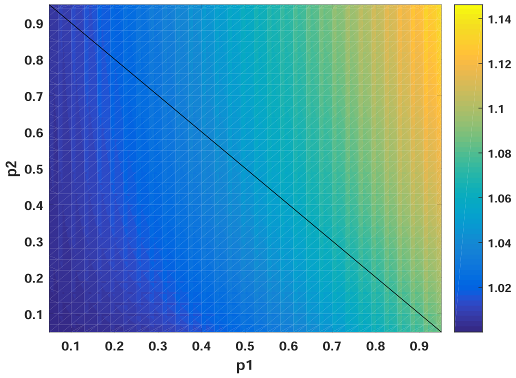

FIGURE 8. When $\delta_1 = 0.8$, the average power incomes of pool 1 in the case of the optimum infiltration.

pool 1 and pool 2 is close to 1, the infiltrate rate of pool 1 is larger. When the value of the miner betrayal rate δ_1 of the mining pool 1 increases, the value of the infiltrate rate a_{12} of mining pool 1 also gradually increases. Fig.3, Fig.6 and Fig.9 are the average power incomes of pool 1 in the case of the optimum infiltration. It has been observed that the profit gained by mining pool 1 when choosing an attack strategy is higher than that when it chooses not to attack, that is, choosing an attack strategy can increase its own revenue. When the total mining power of pool 1 and pool 2 is close to 1, the average power incomes $\overline{R}_1$ of pool 1 is larger. When the value of the miner betrayal rate δ_1 of mining pool 1 increases, the average power incomes of mining pool 1 $\overline{R}_1$ gradually decreases. It means that the more miners betrayed, the more adverse the impact on the profit of mining pool 1. Fig.4, Fig.7 and Fig.10 are the average power incomes of pool 2 in the case of the optimum infiltration. It has been observed that the average power incomes of mining pool 2

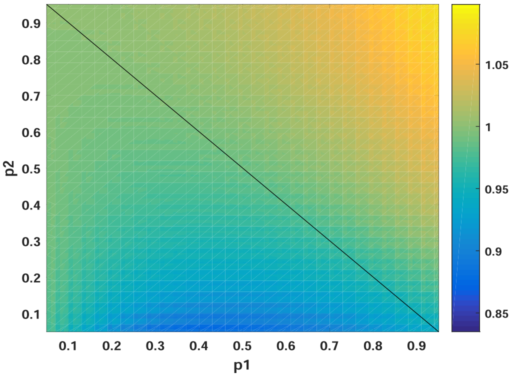

FIGURE 9. When $\delta_1 = 0.8$, the average power incomes of pool 2 in the case of the optimum infiltration.

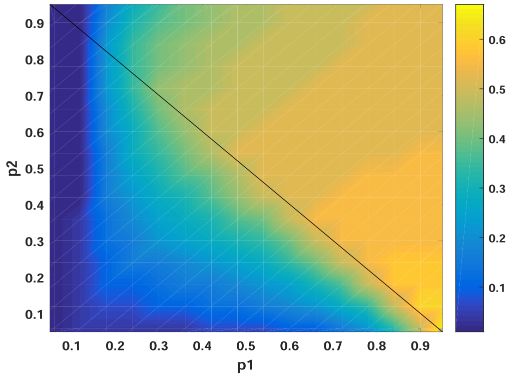

FIGURE 10. When the two mining pools attack each other and δ_1 takes 0.2, the value of a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

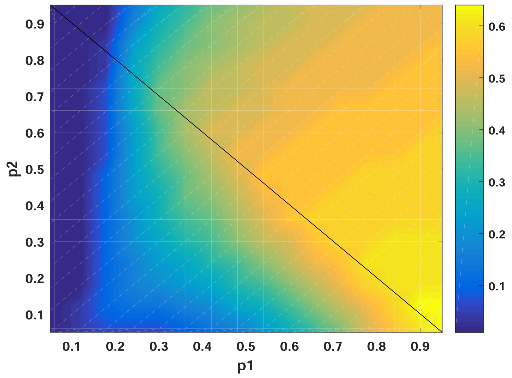

FIGURE 11. When the two mining pools attack each other and δ_1 takes 0.5, the value of a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

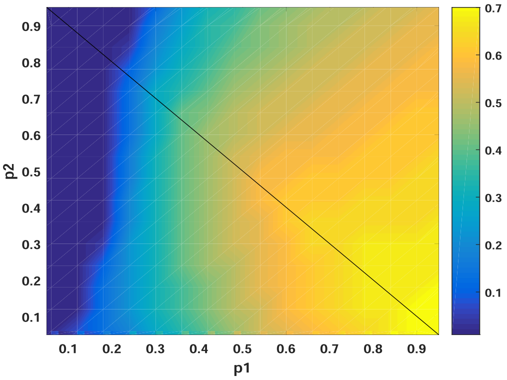

FIGURE 12. When the two mining pools attack each other and δ_1 takes 0.8, the value of a_{12} at the Nash equilibrium in the case of different p_1 and p_2.

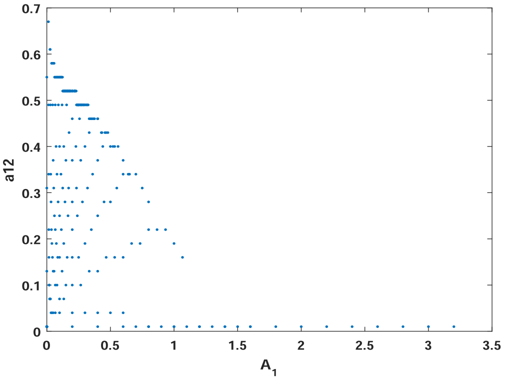

FIGURE 13. When the two mining pools attack each other and δ_1 takes 0.2, the change of a_{12} in Nash equilibrium under different cases of A_1.

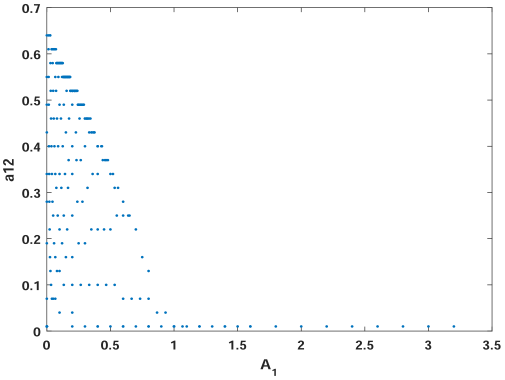

FIGURE 14. When the two mining pools attack each other and δ_1 takes 0.5, the change of a_{12} in Nash equilibrium under different cases of A_1.

is generally lower than that of mining pool 1. This shows that when the opponent's mining pool chooses not to attack the strategy, the attack can increase its own revenue and effectively reduce the revenue of the opposing mining pool. When the total mining power of pool 1 and pool 2 is close to 1, the average power incomes $\overline{R}_2$ of pool 2 is larger. When the value of the miner betrayal rate δ_1 of mining pool 1 increases, although the change trend of the average power income of mining pool 2 is not too obvious, but it also has a slight increase. The results show that the more miners betrayed in mining pool 1, the more effect it will have on the income of mining pool 2. But on the whole, when mining pool 1 chooses to attack, its income is still higher than that of mining pool 2.

Next, we consider the situation where two mining pools attack each other. Fig.11-13 are the values of a_{12} at the Nash equilibrium under the different p_1 and p_2 when δ_1 is taken as

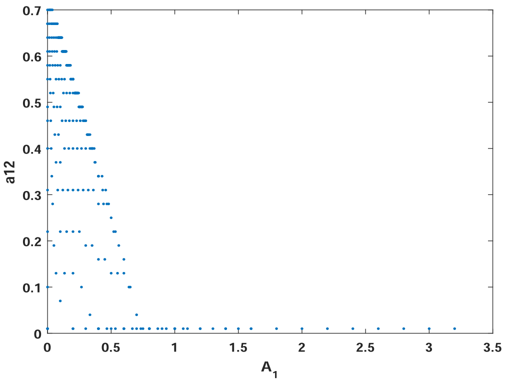

FIGURE 15. When the two mining pools attack each other and δ_1 takes 0.8, the change of a_{12} in Nash equilibrium under different cases of A_1.

0.2, 0.5, 0.8 respectively. It is found through observation that when the total mining power of pool 1 and pool 2 is close to 1, the average power incomes $\overline{R}_1$ of pool 1 is larger. And as δ_1 increases, the value of a_{12} gradually increases. Fig.14-16 are the changes of a_{12} in Nash equilibrium under different cases of A_1 when δ_1 is taken as 0.2, 0.5, 0.8 respectively. Because the computing power of the mining pool varies, the same ratio of the power to be infiltrated A_1 corresponds to multiple optimal infiltrate rates a_{12}. Through observation we found that as the A_1 increases, the infiltrate rates a_{12} of mining pool 1 gradually decreases. On the whole, with the increase of the betrayal rate δ_1, the threshold of the ratio of the power to be infiltrated A_1 decreases gradually when the infiltrate rates a_{12} decreases to 0. And the infiltrate rates a_{12} decreases with the increase of the betrayal rate δ_1 under the same ratio of the power to be infiltrated A_1.

V. CONCLUSION

For existing papers, a mining pool game model based on the PoW consensus mechanism from the perspective of adding rewards and punishments to the blockchain system is builded firstly in this paper. And its pure strategy Nash equilibrium and mixed strategy Nash equilibrium are analyzed. Then the block withholding attacks between mining pools are considered. That is, the infiltrate rate and betrayal rate of the mining pool are considered, related models are builded, the Nash equilibrium and the value of infiltrate rate under the Nash equilibrium are analyzed. This is also a new discussion that has not appeared in other papers. Finally, the influence of the mining pool's computing power, the ratio of the power to be infiltrated, and the betrayed rate of dispatched miners on the mining pool's infiltration rate selection and income are explored by numerical simulation. Nowadays, the upsurge of blockchain technology has swept across all walks of life and has become one of the hottest and most noticed information technologies of the moment. The PoW consensus mechanism has always played a very important role in blockchain technology. The phenomenon of mutual attack of mining pools in blockchain technology has brought a very adverse impact on the application of blockchain technology. This article analyzes the Nash equilibrium from the perspective of adding reward and punishment mechanisms to the blockchain system and block withholding attacks between mining pools, and discusses the value of the infiltrate rate under the maximum profit of the mining pool. It has a certain effect on the research of blockchain technology. However, blockchain technology integrates a variety of complex computer technologies such as encryption algorithms, P2P file transfers, and consensus mechanisms. The research content of this article is relatively single. In the future, game theory will continue to be more deeply integrated with the problems existing in blockchain technology. Based on the model studied in this paper, we will continue to study the mining dilemma in depth, hoping to provide more effective help in improving the promotion of blockchain technology.

REFERENCES

[1] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Autom. Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[2] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Jul. 2017, pp. 763–768.

[3] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, Feb. 2018.

[4] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, May 2018.

[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw.*, Apr. 2015, pp. 184–191.

[6] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, Jun. 2018.

[7] S. Wang, "Research status and innovation trend of block chain technology in the financial field," *Shanghai Finance*, vol. 2016, no. 2, pp. 26–29, 2016.

[8] Y. N. Xu, "Solution analysis of intelligent logistics industry based on blockchain and Internet of Things," *Digital World*, vol. 2018, no. 4, pp. 604–605, 2018.

[9] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, Sep. 2016.

[10] X. G. Wang, "A survey of blockchain technology consensus algorithms," *China Comput. Commun.*, vol. 379, no. 9, pp. 72–74, 2017.

[11] X. Shen, Q. Q. Pei, and X. F. Liu, "Summary of blockchain technology," *J. Netw. Inf. Secur.*, vol. 2, no. 11, pp. 11–20, 2016.

[12] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoin's proof of work via proof of stake [extended abstract]y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[13] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018.

[14] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 195–209.

[15] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proc. 14th Int. Conf. Auto. Agents Multiagent Syst.*, 2015, pp. 919–927.

[16] C. B. Tang, Z. Yang, Z. L. Zheng, and Z. Y. Cheng, "Analysis and optimization of game dilemma in PoW consensus algorithm," *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1520–1531, 2017.

[17] L. Fan, H. Zheng, J. H. Huang, Z. C. Li, and Y. H. Jiang, "Blockchain mining pool cooperative evolution method based on adaptive zero determinant strategy," *J. Comput. Appl.*, vol. 2018, doi: 10.11772/j.issn.1001-9081.2018071619.

[18] T. T. Wang, S. Y. Yu, and B. M. Xu, "Research on PoW mining dilemma based on policy gradient algorithm," *J. Comput. Appl.*, vol. 39, no. 5, pp. 1336–1442, May 2019, doi: 10.11772/j.issn.1001-9081.2018102197.

[19] I. Eyal, "The Miner's dilemma," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2015, pp. 89–103.

[20] S. Y. Chang, Y. H. Park, S. Wuthier, and C. W. Chen, "Uncle-block attack: Blockchain mining threat beyond block withholding for rational and uncooperative miners," in *Proc. ACNS*, 2019, pp. 241–258.

WENBAI LI (Member, IEEE) received the B.Eng. and M.Eng. degrees in information and computing science and the Ph.D. degree in mechanical engineering and automation from Northwestern Polytechnical University, Xi'an, China, in 2006, 2008, 2012, respectively. In 2014, he was with the College of Economics and Management, Zhejiang Normal University, Jinhua, China, where he is currently a Lecturer of computer science. His research interests include blockchain and its applications, networked control systems, and multi-agent systems.

MENGWEN CAO received the bachelor's degree from Anqing Normal University, Anqing, China, in 2017. She is currently pursuing the master's degree with the Department of Mathematics, College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua, China. Her current research interests include game theory and its applications in the blockchain.

YUE WANG is currently pursuing the degree with the Department of Communication Engineering, College of Physics and Electronics Information Engineering, Zhejiang Normal University, Jinhua, China. Her research interests include game theory and its applications in the blockchain.

CHANGBING TANG (Member, IEEE) received the B.S. and M.S. degrees in mathematics and applied mathematics from Zhejiang Normal University, Jinhua, China, in 2004 and 2007, respectively, and the Ph.D. degree from the Department of Electronics Engineering, Fudan University, Shanghai, China, in 2014. He is currently an Associate Professor with the College of Physics and Electronics Information Engineering, Zhejiang Normal University. His current research interests include game theory, blockchain and its applications, and networks and distributed optimization. He was a recipient of the Academic New Artist Doctoral Post Graduate from the Ministry of Education, China, in 2012.

FEILONG LIN (Member, IEEE) received the B.Eng. and M.Eng. degrees in electronics information engineering from Xidian University, Xi'an, China, in 2004 and 2007, respectively, and the Ph.D. degree in control science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2016. He joined the College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua, China, in 2016, where he is currently a Lecturer and the Associate Director of the Department of Computer Science and Engineering. His research interests include blockchain and its applications, the Internet of Things, and industrial automation.