Proceedings of the 38th Chinese Control Conference
July 27-30, 2019, Guangzhou, China

Application of ZD Strategy in Mining Pool Game

Mengwen Cao, Changbing Tang*, Yang Liu, Feilong Lin, Zhongyu Chen
Academy of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321000, China.
E-mail: tangcb@zjnu.cn

Abstract: Blockchain is a decentralized billing system that guarantees mutual trust among parties through decentralized data storage, sophisticated encryption and signature technologies. The basis of blockchain is P2P distributed network, encryption algorithm and consensus mechanism. To improve the reward during the process of mining, the mining pool will choose to cooperate or attack with other mining pools. In this paper, the zero-determinant (ZD) strategy is applied to to optimize the strategy selection during the mining process, which enforces mining pools selecting cooperative mining and thereby increase the overall revenue of the pools. In addition, numerical illustrations are also presented to support our theoretical analysis.

Key Words: Blockchain, ZD strategy, mining game, infiltrate rate

1 Introduction

The formal proposal of blockchain technology can be traced back to the idea of a bitcoin in 2008 by a scholar named Nakamoto Satoshi, which is a distributed ledger technology in P2P networks. The advantage of blockchain technology lies in the decentralized design. It realizes point-to-point transaction based on decentralized credit in a distributed network where nodes do not need to trust by using encryption algorithm, time stamp, tree structure, consensus mechanism and reward mechanism. Blockchain technology is not a single, completely new technology, but the integration of various existing technologies, such as encryption algorithms, P2P file transfer, and consensus mechanisms. These technologies are skillfully combined with databases to form a new way of data recording, delivery, storage and presentation. Among them, the consensus mechanism has a very important position in the blockchain technology, which allows the whole network nodes reaching a consensus and create a trust-free accounting mechanism on the blockchain [1].

Bitcoin system applies blockchain as the underlying framework supporting technology of the system, and achieves the irreparable modification and unforgeability of transactions through the consensus mechanism of Proof of Work (PoW) [2]. The core idea of the PoW consensus mechanism is to ensure data consistency and consensus security by introducing computational power competition of distributed nodes. Specifically, each node uses its own computing power to compete with each other to solve a SHA256 mathematical problem that is complex but easy to verify [3]. The node that first completes the problem will obtain the transaction billing right and obtain certain rewards. In a bitcoin system, the implementation of PoW produces a block. The process of producing the block is also known as mining and the nodes are called miners [4]. According to the bitcoin system, a block is created every 10 minutes, which means that a miner with very little mining power may not be rewarded for a long time if he mines alone, so the miners choose to join the pool.

A pool consists of a pool manager and a number of miners, in which miners use computational power to mine and obtain a return proportional to the computational power sending to the manager. The sending part of the work proves to be no value for the bitcoin system, and can only be used as a yardstick to measure the miners' contribution to the calculation, i.e. the miners do not contribute to the effective calculation but gain some of the profits from the pool. This behavior is called block withholding attack [9]. In a pool, miners can intercept and attack the pool, sharing the benefits of the pool with other miners. However, the pool can also use miners to infiltrate into other pools, and block interception attacks on other pools [7]. In the PoW consensus process, the pool dilemma corresponds to the classical prisoner dilemma model [17]. The Nash equilibrium of the pool dilemma model is mutual attack. However, the benefit of pool-to-pool mutual attack is less than that of no attack, which means that the system is not optimal. To improve the overall benefits of the system, it is necessary to establish relevant mechanisms to make the pool tend to cooperate [10, 16, 18, 19].

Zero determinant (ZD) strategy [5, 6] is a new method rising in the game theory in recent years. It can break the traditional Nash equilibrium theory and optimize the system income [8]. Whatever strategy the opponent adopts, the party adopting the ZD strategy can not only control the opponent's income[20], but also force the opponent to have a linear relationship with his own income to achieve the optimal system [11–15]. In this paper, we will use ZD strategy in the pool game to optimize the system benefits, and ultimately get higher returns.

The organizational structure of this paper is as follows: The two-pool game is described in Section 2. The algorithm of zero-determinant strategy is given in Section 3. Section 4 carries on the data simulation and the result analysis, which indicates that the ZD strategy can effectively improve the overall income. We summarizes our work in Section 5.

2 System model

In the process of mining, a pool can gain profit by the power contributed by the pool members. Let the power of the two mining pools is p_1,p_2 and $0 < p_i < 1, i = 1, 2, 0 < p_1 + p_2 \leq 1$. Without loss of generality, set the total revenue $R = 1$. When the pool chooses to cooperate, it gets the m reward, and when it chooses to attack, it gets the $km(0 \leq m \leq 1, k \geq 1)$ punishment, where k is the proportion of the punishment to the reward. $d(d \geq 0)$ is the profit of the pool

This work was partly supported by the Key Projects of National Natural Science Foundation of China (No.61751303), and the Zhejiang Provincial Natural Science Foundation of China (Nos.LY16F030002 and LY18F030013).

that chooses to attack, d' (d' can be positive or negative) is the final income of the mining pool when all pools choose to attack. There is the situation of their payoff (see Table 1).

Table 1: Payoff of Pool

	N	A
N	p_1, p_2	p_1+m-d, p_2-km+d
A	p_1-km+d, p_2+m-d	p_1-km-d', p_2-km+d'

The payoff of pool $i(i=1,2)$ is $p_i \cdot 1 = p_i$ when both pools choose N (Not to attack), that is, they do not send miners into each other's pool. When one pool chooses not to attack and the other chooses to A(Attack), the pool that chooses not to attack will get a reward m, but will lose d revenue, its revenue is $p_i + m - d(i = 1, 2)$, the pool that chooses to attack will be punished km, and get d revenue from the pool that is attacked, its revenue is $p_i - km + d(i = 1, 2)$. When all pools choose to attack, the income of pool i is $p_i + m \pm d'(i = 1, 2)$.

Next, we discuss the Nash equilibrium of the strategy.

- When $m < d' < d < km$ and $m - d < d' - km < d - km$. 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 $d > d' > km$. 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 $d' < d < m$ and $m-d > 0, d'-km < d-km < 0$. 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 $m < d' < d < km$ and $m - d < d' - km < d - km$, 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.

3 Game optimization with ZD strategies

In the two-pool repeated game, the mining pool that chooses the attack strategy will send its own loyal miners to another mining pool to carry out block withholding attacks to gain income, thereby increasing the income of its own pool. We use $r_{i,j}, i, j = 1, 2$ to indicate the infiltrate ratio of the mining pool i to the mining pool j, and $r_{i,i}$ is the power ratio of the mining pool itself, and $\sum_{j=1}^{2} r_{i,j} = 1$, $0 \le r_{i,j} < 1, i = 1, 2$. The two-pool game model can be regarded as the iterative prisoner dilemma model. The pool can choose attack and non-attack strategies, which correspond to competition and cooperation respectively. Therefore, the probability of selecting the cooperation of the mining pool i is $r_{i,i}$, and the probability of selecting the attack is $r_{i,j}$. In each round of the game, each mining pool has four conditions: (N, N), (N, A), (A, N), (A, A). The mixed strategy choices for mining pool 1 and mining pool 2 are $\mathbf{r_1} = (r^1_{1,1}, r^2_{1,1}, r^3_{1,1}, r^4_{1,1})$ and $\mathbf{r_2} = (r^1_{2,2}, r^2_{2,2}, r^3_{2,2}, r^4_{2,2})$. $\mathbf{r_1}$ and $\mathbf{r_2}$ are the change vectors for selecting the N strategy in the next round of game, ie, $r^1_{1,1}$ is the probability that pool 1 choose N strategy in the next round of game when pool 1 and the pool 2 choose N strategy in the current game, the probability of selecting the A strategy is $1-r^1_{1,1}$, that is, $r^1_{1,2}$. The probability that the mining pool 2 selects the strategy N is $r^1_{2,2}$, and the A strategy is selected with the probability of $1-r^1_{2,2} = r^1_{2,1}$. Similarly, $r^2_{1,1}, r^3_{1,1}$ and $r^4_{1,1}$ are respectively expressed as the probability of selecting N strategy of pool 1 in the next round of game when the behavior of the pool 1 is (N, A), (A, N), (A, A) in the current game, the probability of choosing A strategy is $r^2_{1,2}, r^3_{1,2}, r^4_{1,2}$. $r^2_{2,2}, r^3_{2,2}$ and $r^4_{2,2}$ are respectively expressed as the probability of selecting N strategy of pool 2 in the next round of game when the behavior of the pool 2 is (A, N), (N, A), (A, A) in the current game, the probability of choosing A strategy is $r^2_{2,1}, r^3_{2,1}, r^4_{2,1}$. The income vector of pool 1 is:

$$\mathbf{w^1} = (w^1_1, w^1_2, w^1_3, w^1_4) = (p_1, p_1+m-d, p_1-km+d, p_1-km-d'), \tag{1}$$

The income vector of pool 2 is:

$$\mathbf{w^2} = (w^2_1, w^2_2, w^2_3, w^2_4) = (p_2, p_2-km+d, p_2+m-d, p_2-km+d'), \tag{2}$$

The process of the repeated game between the mining pool 1 and the mining pool 2 can be represented by a Markov chain, and the corresponding probability transfer matrix is:

$$M = \begin{pmatrix} r^1_{1,1}r^1_{2,2} & r^1_{1,1}r^1_{2,1} & r^1_{1,2}r^1_{2,2} & r^1_{1,2}r^1_{2,1} \\ r^2_{1,1}r^3_{2,2} & r^2_{1,1}r^3_{2,1} & r^2_{1,2}r^3_{2,2} & r^2_{1,2}r^3_{2,1} \\ r^3_{1,1}r^2_{2,2} & r^3_{1,1}r^2_{2,1} & r^3_{1,2}r^2_{2,2} & r^3_{1,2}r^2_{2,1} \\ r^4_{1,1}r^4_{2,2} & r^4_{1,1}r^4_{2,1} & r^4_{1,2}r^4_{2,2} & r^4_{1,2}r^4_{2,1} \end{pmatrix}$$

Because the M matrix has a characteristic vector whose eigenvalues are one. Let $M' = M - I$, then M' is irreversible, and the determinant is equal to zero. Define the steady-state distribution vector of the M matrix as $\mathbf{v}$, $\mathbf{v} = (v_1, v_2, v_3, v_4)^T$ and $\sum_{i=1}^{4} v_i = 1$, then

$$\mathbf{v}^T \cdot M = \mathbf{v}^T, \tag{3}$$

i.e.

$$\mathbf{v}^T M' = 0. \tag{4}$$

It is known from the properties of Kramm's law and the adjoint matrix:

$$Adj(M')M' = det(M')I, \tag{5}$$

then each row of $Adj(M')$ is linearly related to $\mathbf{v}^T$. We select any vector of four elements $\mathbf{f} = (f_1, f_2, f_3, f_4)^T$, and it can be obtained by Laplace transform:

$$\begin{aligned} \mathbf{v}^T \cdot \mathbf{f} &\equiv D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{f}) \\ &= det \begin{pmatrix} -1+r^1_{1,1}r^1_{2,2} & -1+r^1_{1,1} & -1+r^1_{2,2} & f_1 \\ r^2_{1,1}r^3_{2,2} & -1+r^2_{1,1} & r^3_{2,2} & f_2 \\ r^3_{1,1}r^2_{2,2} & r^3_{1,1} & -1+r^2_{2,2} & f_3 \\ r^4_{1,1}r^4_{2,2} & r^4_{1,1} & r^4_{2,2} & f_4 \end{pmatrix}. \end{aligned} \tag{6}$$

The second column and the third column of the determinant are separately controlled by the mining pool 1 and the mining pool 2. By the nature of the Markov chain, the payoff of the pools at steady state are:

$$e^1 = \frac{\mathbf{v}^T \cdot \mathbf{w^1}}{\mathbf{v}^T \cdot \mathbf{1}} \equiv \frac{D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{w^1})}{D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{1})}, \tag{7}$$

$$e^2 = \frac{\mathbf{v}^T \cdot \mathbf{w^2}}{\mathbf{v}^T \cdot \mathbf{1}} \equiv \frac{D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{w^2})}{D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{1})}. \tag{8}$$

Let $f = \alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1}$ (α, β and γ are parameters), then:

$$\begin{aligned} \alpha e^1 + \beta e^2 - \gamma \cdot 1 &= \frac{\mathbf{v}^T \cdot (\alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})}{\mathbf{v}^T \cdot \mathbf{1}} \\ &\equiv \frac{D(\mathbf{r_1}, \mathbf{r_2}, \alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})}{D(\mathbf{r_1}, \mathbf{r_2}, \mathbf{1})}. \end{aligned} \tag{9}$$

Let $r_1' = (-1 + r_{1,1}^1, -1 + r_{1,1}^2, r_{1,1}^3, r_{1,1}^4)$, $r_2' = (-1 + r_{2,2}^1, r_{2,2}^3, -1 + r_{2,2}^2, r_{2,2}^4)$, if the mixing strategy of the pool 1 satisfies $r_1' = \phi(\alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})$, ϕ is a non-zero parameter, or the mixing strategy of the pool 2 satisfies $r_2' = \phi(\alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})$, then:

$$\alpha e^1 + \beta e^2 - \gamma = 0 \tag{10}$$

We call the strategy adopted by pool 1 or pool 2 as zero determinant strategy. It can be seen from the formula that when one of the pools adopts zero determinant strategy, no matter what strategy the other side adopts, it can always keep a linear relationship between the expected returns of the two pools and satisfy $\gamma = \alpha e^1 + \beta e^2$.

Corollary 1. *Assuming that pool 1 adopts a zero determinant strategy, the parameters α and β satisfy:*

$$-1 \le \frac{\alpha}{\beta} < 0, \tag{11}$$

parameter γ satisfies:

$$\gamma \le \min\{\alpha p_1 + \beta p_2, \alpha(p_1 + m - d) + \beta(p_2 - km + d)\}, \tag{12}$$

$$\begin{aligned} \gamma \ge \max\{&\alpha(p_1 - km + d) + \beta(p_2 + m - d), \\ &\alpha(p_1 - km - d') + \beta(p_2 - km + d')\}. \end{aligned} \tag{13}$$

Proof. According to $Eq.(10)$, $\frac{\alpha}{\beta} < 0$, when pool 1 adopts zero determinant strategy, it needs to satisfy $r_1' = \phi(\alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})$, that is:

$$\begin{aligned} \begin{pmatrix} -1 + r_{1,1}^1 \\ -1 + r_{1,1}^2 \\ r_{1,1}^3 \\ r_{1,1}^4 \end{pmatrix} = \phi[&\alpha \begin{pmatrix} p_1 \\ p_1 + m - d \\ p_1 - km + d \\ p_1 - km - d' \end{pmatrix} + \beta \begin{pmatrix} p_2 \\ p_2 - km + d \\ p_2 + m - d \\ p_2 - km + d' \end{pmatrix} \\ &- \gamma \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}]. \end{aligned} \tag{14}$$

The probability $r_{1,1}^i (i = 1, 2, 3, 4)$ of the hybrid strategy needs to satisfy $0 \le r_{1,1}^i \le 1$, which is:

$$\begin{cases} 0 \le r_{1,1}^1 = \phi(\alpha p_1 + \beta p_2 - \gamma) + 1 \le 1 \\ 0 \le r_{1,1}^2 = \phi[\alpha(p_1 + m - d) + \beta(p_2 - km + d) - \gamma] + 1 \le 1 \\ 0 \le r_{1,1}^3 = \phi[\alpha(p_1 - km + d) + \beta(p_2 + m - d) - \gamma] \le 1 \\ 0 \le r_{1,1}^4 = \phi[\alpha(p_1 - km - d') + \beta(p_2 - km + d') - \gamma] \le 1 \end{cases} \tag{15}$$

In the Eq.(15), when $\phi > 0$, there are:

$$\gamma \ge \max\{\alpha p_1 + \beta p_2, \alpha(p_1 + m - d) + \beta(p_2 - km + d)\} \tag{16}$$

$$\begin{aligned} \gamma \le \min\{&\alpha(p_1 - km + d) + \beta(p_2 + m - d), \\ &\alpha(p_1 - km - d') + \beta(p_2 - km + d')\}. \end{aligned} \tag{17}$$

In the mining pool game model, there is $p_1 - km + d \ge p_1 + m - d$, $p_2 - km + d \ge p_2 + m - d$. Without loss of generality, assuming $\alpha < 0, \beta > 0$, then

$$\alpha(p_1 + m - d) + \beta(p_2 - km + d) \ge \alpha(p_1 - km + d) + \beta(p_2 + m - d). \tag{18}$$

Obviously, inequality (18) is incompatible with inequality (16) and (17).

When $\phi < 0$,

$$\gamma \le \min\{\alpha p_1 + \beta p_2, \alpha(p_1 + m - d) + \beta(p_2 - km + d)\} \tag{19}$$

$$\begin{aligned} \gamma \ge \max\{&\alpha(p_1 - km + d) + \beta(p_2 + m - d), \\ &\alpha(p_1 - km - d') + \beta(p_2 - km + d')\}. \end{aligned} \tag{20}$$

By inequality (19), (20), it is necessary to satisfy

$$\alpha(p_1 - km - d') + \beta(p_2 - km + d') \le \alpha p_1 + \beta p_2, \tag{21}$$

namely,

$$\frac{\alpha}{\beta} \ge \frac{-(-km + d')}{-km - d'} \ge \frac{-(-km - d')}{-km - d'} = -1. \tag{22}$$

In summary, when the mining pool 1 adopts the zero determinant strategy, that is,$r_1' = \phi(\alpha\mathbf{w^1} + \beta\mathbf{w^2} - \gamma \cdot \mathbf{1})$, the parameters α, β satisfy the inequality (11), and the parameter γ satisfies the inequalities (12) and (13). □

Corollary 2. *When $\alpha = 0$, the pool 1 adopts the ZD strategy to satisfy $r_1' = \phi(\beta\mathbf{w^2} - \gamma \cdot \mathbf{1})$, and $\beta e^2 - \gamma = 0$, it can be launched:*

$$\begin{cases} r_{1,1}^1 = \phi(\frac{p_2}{e^2} - 1)\gamma + 1 \\ r_{1,1}^2 = \phi(\frac{p_2 - km + d}{e^2} - 1)\gamma + 1 \\ r_{1,1}^3 = \phi(\frac{p_2 + m - d}{e^2} - 1)\gamma \\ r_{1,1}^4 = \phi(\frac{p_2 - km + d'}{e^2} - 1)\gamma \end{cases}. \tag{23}$$

Theorem 1. *When the pool 1 adopts zero determinant strategy to achieve maximum overall payoff, we can get specific zero determinant strategy as follows:*

$$\begin{cases} r_{1,1}^1 = 1 \\ r_{1,1}^2 = \phi[\alpha(m - d) + \beta(-km + d)] + 1 \\ r_{1,1}^3 = \phi[\alpha(-km + d) + \beta(m - d)] \\ r_{1,1}^4 = \phi[\alpha(-km - d') + \beta(-km + d')] \end{cases}. \tag{24}$$

Under this strategy choice, the profit of the two pools can reach a higher value, and the total income can reach up to $w = w_1^1 + w_1^2$.

Proof. Let $e^1 = w_1^1$, $e^2 = w_1^2$, it can be proved by combining with Eq.(10) and Eq.(14). □

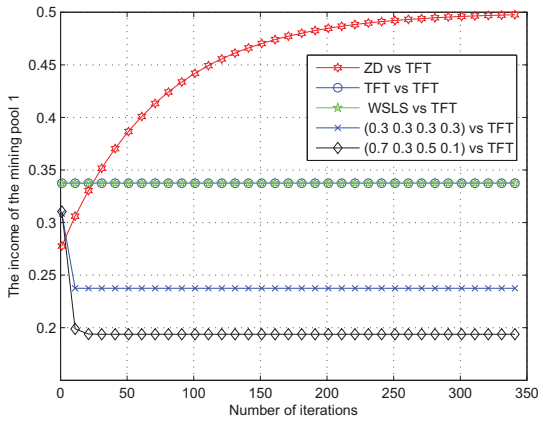

Fig. 1: The income of the mining pool 1 when the mining pool 1 adopts other strategies and mining pool 2 adopts TFT strategy.

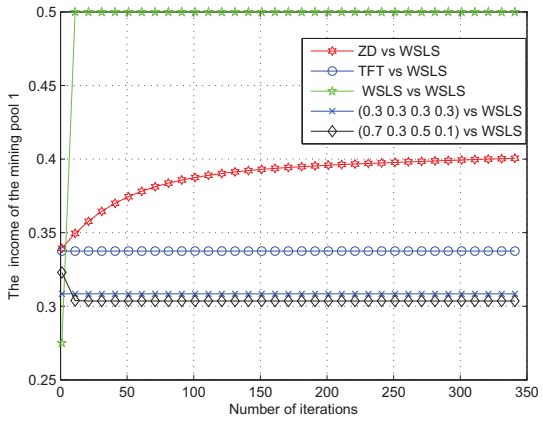

Fig. 2: The income of the mining pool 1 when the mining pool 1 adopts other strategies and mining pool 2 adopts WSLS strategy.

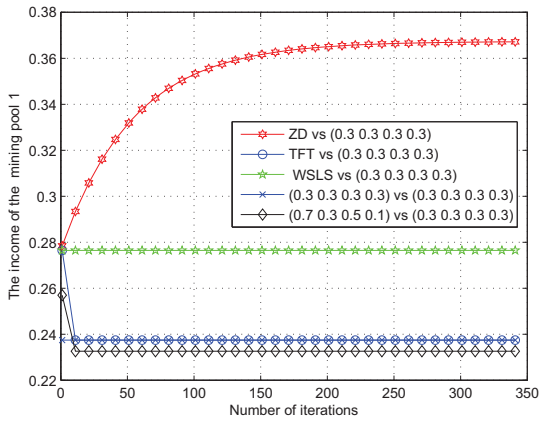

Fig. 3: The income of the mining pool 1 when the mining pool 1 adopts other strategies and mining pool 2 adopts (0.3,0.3,0.3,0.3) strategy.

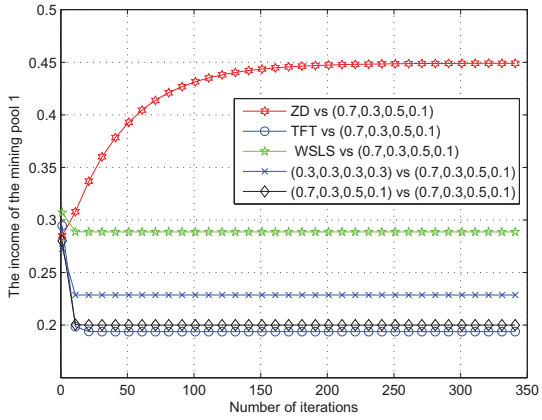

Fig. 4: The income of the mining pool 1 when the mining pool 1 adopts other strategies and mining pool 2 adopts (0.7,0.3,0.5,0.1) strategy.

4 Numerical simulation and result analysis

Based on the two-pool game model analysis in Section 3, this section will verify the feasibility of adopting the ZD strategy in the mining pool through numerical simulation, that is, what the infiltrate ratio of the mining pool is controlled, the highest profit can be achieved. The main experimental tool used in this section is Matlab. The mining pool adopts zero determinant strategy to control its own linear relationship with the counterpart's income. The relevant parameters are set as follows: the mining pool get the reward $m = 0.1$ for choosing not to attack, and the ratio of punishment to reward is $k = 3$, then $km = 0.3$, in addition, $d = 0.28$, $d' = 0.15$, $\phi = -\frac{1}{45}$, $\alpha = -1$,$\beta = 7$. Let us first consider the case where the two mining pools have the same power, assuming $p_1 = 0.5$, $p_2 = 0.5$.

In Fig.1, the mining pool 2 has always adopted the TFT strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy, (0.7,0.3,0.5,0.1) strategy. We can see that the payoff of the mining pool 1 can reach a better value after a certain iteration when it adopts the ZD strategy, but the other four strategies can not. In addition, when the mining pool 1 adopts the TFT and WSLS strategy, the change trend of their income are completely similar in the iterative process.

In Fig.2, the mining pool 2 has always adopted the WSLS strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy,(0.7,0.3,0.5,0.1) strategy. From the image we can see that when both the mining pool 1 and the mining pool 2 use the WSLS strategy, the payoff of the mining pool 1 is the lowest at the beginning, but after several iterations, it reaches the highest value very quickly. Although after some iterations, the mining pool 1 can achieve a higher return when using the ZD strategy, but it is lower than the gain from using the WSLS strategy. This shows that the adoption of the ZD strategy does not necessarily lead to the highest value of revenue, but only to achieve a better value. Obviously, in this case, adopting the WSLS strategy is the best choice.

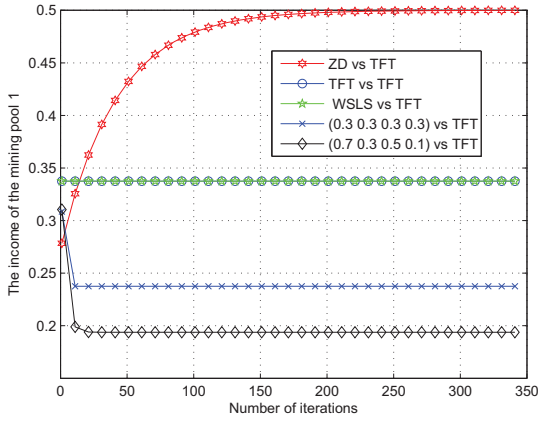

Fig. 5: The income of the pool 1 when it adopts other strategies and pool 2 adopts TFT strategy.

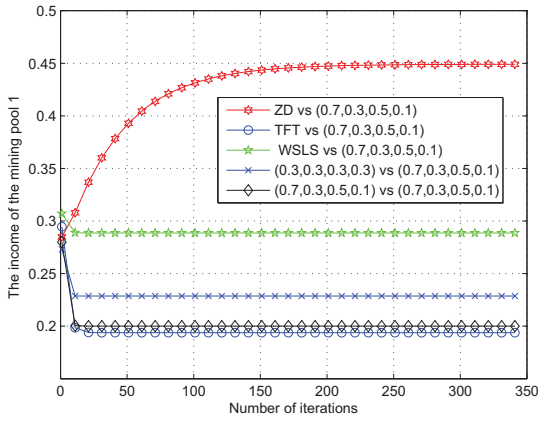

Fig. 6: The income of the pool 1 when it adopts other strategies and pool 2 adopts (0.7,0.3,0.5,0.1) strategy.

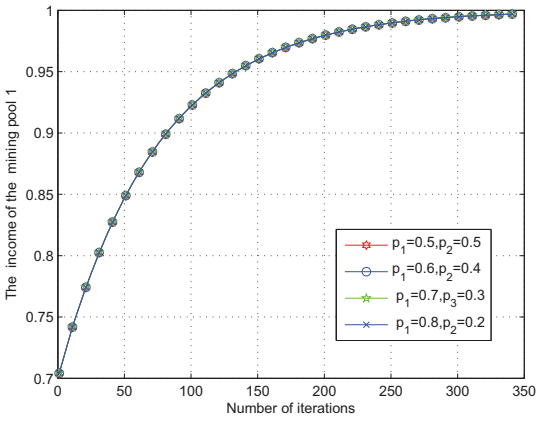

Fig. 7: The total income of the mining pools when the initial power of the pools are different.

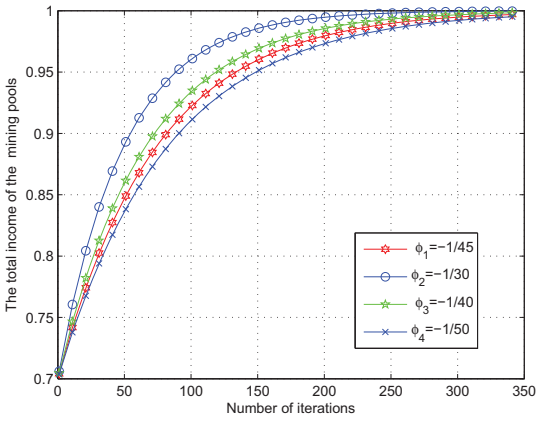

Fig. 8: The total income of the mining pool 1 when the initial power of the pools are different.

In Fig.3, the mining pool 2 has always adopted the (0.3,0.3,0.3,0.3) strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy, (0.7,0.3,0.5,0.1) strategy. By comparison, the mining pool 1 has a significant advantage over the other four strategies when adopting the ZD strategy, although these five strategic choices can not make the income of the mining pool 1 reach the highest value. What's more, there is a tendency to reduce revenue when the mining pool adopts TFT and (0.7, 0.3, 0.5, 0.1) strategy. When the mining pool 1 adopts the ZD strategy, the WSLS strategy and the TFT strategy, the initial benefits are equal, but after iteration, it develops toward three different trends. In Fig.4, the mining pool 2 has always adopted the (0.7,0.3,0.5,0.1) strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy, (0.7,0.3,0.5,0.1) strategy. In the beginning, the benefits obtained by the five strategies are similar, but after several iterations, only when the ZD strategy is adopted, the trend of the payoff of the mining pool 1 is gradually increasing and reaching a better value. The other four strategies all have a downward trend change. By comparing several sets of simulation results, we find that the ZD strategy adopted by the mining pool in the game process can not guarantee the highest return, but it can always keep the income within a better range. Therefore, in order to achieve a better profit , the ZD strategy is indeed a good choice.

Next, let's make $\alpha = 0$ and observe the change of benefit of the mining pool 1 through simulation results. In Fig.5, the mining pool 2 has always adopted the TFT strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy, (0.7,0.3,0.5,0.1) strategy. Comparing Fig.5 with Fig.1, the overall revenue change of the mining pool 1 does not change much. However, the speed of achieving the optimal income is faster than that of $\alpha = -1$, when the mining pool 1 adopts the ZD strategy. In Fig.6, the mining pool 2 has always adopted the (0.7,0.3,0.5,0.1) strategy, and the mining pool 1 adopts the ZD strategy, TFT strategy, WSLS strategy, (0.3,0.3,0.3,0.3) strategy, (0.7,0.3,0.5,0.1) strategy. Comparing Fig.6 with Fig.4, when the mining pool 1 adopts the ZD strategy, the speed of achieving the optimal return is faster than $\alpha = -1$, and the optimal income is also relatively high. There are

no major differences in the profit changes of the other four strategic choices.

In Fig.7, we use simulation results to observe whether the unequal initial power of the pools affect the total return. In the case of setting different initial power of the mining pools, the mining pool 1 adopts the ZD strategy, and the mining pool 2 adopts the TFT strategy. We find that different initial power do not affect the change in the total income of the two pools. Under the setting of four different initial powers, the total income of the mining pool can reach the highest. Finally, we take different values for the parameter ϕ and observe the impact on the total income of the pools. In Fig.8, let ϕ be equal to four groups of different numbers. Through the simulation results, we find that the value of ϕ affects the speed of reaching the highest returns, but does not affect the final returns, and the greater the ϕ value, the faster the maximum returns are achieved. That is to say, the value of ϕ is positively correlated with the speed at which the optimal value of the income is reached.

5 Conclusions

In this paper, we have proposed ZD strategy algorithm to optimize the strategy selection of the mining pool. In terms of the ZD strategy, we can control the other party's revenue and promote the total revenue of the two mining pools. We have found that the speed at which the mining pool adopts the ZD strategy to reach the optimal value when $\alpha = 0$ is greater than when $\alpha = -1$. Further, regardless of the initial power of the mining pool, it does not affect the optimization of the mining pool strategy selection by the ZD strategy algorithm.

Block chain technology is widely used in today's society, and has a good development prospects. PoW consensus mechanism plays a very important role in block chain technology. When nodes attack each other, it will affect the security of block chain technology. In this paper, the ZD strategy is applied in the mining pool game, which can optimize the choice of mining pool, promote the cooperation of the mining pool, and improve the system revenue. In addition, blockchain technology brings together decentralized, decentralized data storage, consensus mechanisms, mature encryption, signature and other computer technologies. This paper studies the problems in consensus mechanism, but there are still more directions for the whole block chain technology to be discussed in depth.

References

[1] Y. Yuan, F. Y. Wang, Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, 42(4): 481-494.

[2] C. B. Tang, Z. Yang, Z. L. Zheng, Z. Y. Cheng, Analysis and optimization of game dilemma in PoW consensus algorithm. *Acta Automatica Sinica*, 2017, 43(9): 1520-1531.

[3] M. Swan, Blockchain thinking: the brain as a decentralized autonomous corporation. *IEEE Technology and Society Magazine*, 2015, 34(4): 41-52.

[4] I. Eyal, The Miner's Dilemma. *Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP)*, 2015: 89-103.

[5] A. Al. Daoud, G. Kesidis, J. Liebeherr, Zero-determinant strategies: a game-theoretic approach for sharing licensed spectrum bands. *IEEE Journal on Selected Areas in Communications*, 2014, 32(11): 2297-2308.

[6] W. H. Press, F. J. Dyson, Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent. *Proceedings of the National Academy of Sciences*, 2012, 109(26): 10409-10413.

[7] W. Mason, D. J. Watts, Financial incentives and the performance of crowds, *ACM SIGKDD Explorations Newsletter*, 11(2): 100-108, Dec. 2010.

[8] C. Hilbe, B. Wu, A. Traulsen, M. A. Nowak, Evolutionary performance of zero-determinant strategies in multiplayer games. *Journal of Theoretical Biology*, 2015, 374: 115-124.

[9] N. T. Courtois, L. Bahack, On subversive miner strategies and block withholding attack in bitcoin digital currency. *Cryptography and Security*, arXiv:1402.1718, 2014.

[10] X. J. Liu, W. B. Wang, D. Niyato, N. Zhao and P. Wang, Evolutionary Game for Mining Pool Selection in Blockchain Networks. *IEEE Wireless Communications Letters*, 7(5): 760-763, Oct. 2018.

[11] H. Q. Zhang, D. Niyato, L. Y. Song, T. Jiang and Z. Han, Equilibrium analysis for zero-determinant strategy in resource management of wireless network. *IEEE Wirel. Commun. Net. Conf.*, Istanbul, pp. 2002-2007, 2015.

[12] H. Q. Zhang, D. Niyato, L. Y. Song, T. Jiang and Z. Han, Zero-determinant Strategy for Resource Sharing in Wireless Cooperations. *IEEE T. Wirel. Commun.*, 15(3): 2179-2192, Mar. 2016.

[13] X. He, H. Dai, P. Ning and R. Dutta, Zero-determinant Strategies for Multi-player Multi-action Iterated Games. *IEEE Signal Proc. Let.*, 23(3): 311-315, Mar. 2016.

[14] L. Pan, D. Hao, Z. H. Rong, T. Zhou, Zero-determinant strategies in iterated public goods game. *Sci. Rep.*, 5(13096), Feb. 2015.

[15] D. Hao, Z. Rong, T. Zhou, Zero-determinant strategy: An underway revolution in game theory. *Chinese Physics B*. 2014, 23(7):164-170.

[16] Z. H. Rong, H. X. Yang, W. X. Wang, Feedback reciprocity mechanism promotes the cooperation of highly clustered scale-free networks. *Physical Review E Statistical Nonlinear & Soft Matter Physics*, 2010, 82(4):047101.

[17] C. Hilbe, M. A. Nowak, K. Sigmund, Evolution of extortion in iterated prisoner's dilemma games. *Proc. Natl. Acad. Sci. USA*, 110(17): 6913-6918, May 2013.

[18] P. Michiardi, R. Molva, CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, *in Proc. IFIP. TC6/TC11 6th Conf. Commun. Mul. Sec. (CMS)*, DOI: 10.1007/978-0-387-35612-923, pp. 107-121, Sep 2002.

[19] C. B. Tang, X. Li, Z. Wang, and J. M. Han, Cooperation and distributed optimization for the unreliable wireless game with indirect reciprocity, *Sci China Inf Sci*, 60(11): 110205, Nov. 2017.

[20] Y. Miao, C. B. Tang, J. F. Lu, X. Li, Zero-determinant strategy for cooperation enforcement in crowdsourcing, *Proc. 2th IEEE Inter. Conf. Data Sci. in Cyb.*,DOI: 10.1109/DSC.2017.42, pp. 1-7, 2017.