Proceedings of the 36th Chinese Control Conference
July 26-28, 2017, Dalian, China

Zero-determinant Strategy for the Algorithm optimize of Blockchain PoW Consensus

Yang Zhen, Miao Yue, Chen Zhong-yu [*], Tang Chang-bing, Chen Xin

College of Mathematics, Physics & Information Engineering, Zhejiang Normal University, Jinhua, 321004
E-mail: czy@zjnu.cn

Abstract: The Proof of Work (PoW) consensus algorithm guarantees the safety and dependability of Blockchain systems. Miners can achieve a consensus through the PoW algorithm during the mining process, that is mutual attacking. However, when the miners attack each other, all miners earn less. In this paper, we established a model that mining between two miners is an iterative game, and proposed a subclass of ZD strategy (a pining strategy) to alleviate miners' dilemma, a miner can control another miner's payoff and increase the social revenue through a pinning strategy. Numerical simulation results verify the effectiveness of the proposed strategy. In summary, this work leads to the better understanding and analysis of the PoW algorithm via the game theory, rendering it possible to design a more rational consensus algorithm in the future.

Key Words: Blockchain, Consensus algorithm, PoW, Iterative game, ZD strategy

1 Introduction

The blockchain is a distributed shared ledger [1], maintained by all the participants in bitcoin system [2]. As the most successful application of blockchain, bitcoin relies on the participation in the PoW consensus of distributed network nodes to complete the verification and record of transactions [3], it also products a set of database with sequential, not be tampered and trustworthy [4]. Through complicated checking mechanism, blockchain database can maintain the integrity, continuity and consistency of data, even if some participants make mistakes, they cannot change blockchain integrity, and tamper with the trading data yet. In brief, blockchain technology [5] involving key points include: decentralized, trustless, collectively maintain, reliable database, time stamp, asymmetric cryptography, and so on.

The PoW is a kind of incentive mechanism in blockchain, and the core concept of PoW is to guarantee the consistency of data and the safety of consensus through the power competition of miners, namely, mining. In bitcion system, nodes competition with each other based on the power of them respective mine, to collectively work out a SHA256 mathematical problems which is solved complicated but easily verified, the node fastest to solve complex problems will acquire the right of recording block and the currency reward with the system automatically generate bitcions, that is this node successfully mines a block.

In the bitcoin system, miners are the participants that mine blocks. It is vulnerable for the open pool since each miner can join this pool by providing a network ID number. Because the currency system produces a block in about 10 minutes, it is extremely difficult for most of the miners to produce a block during a certain period of time. In order to increase the likelihood of stable revenues, many miners choose to join an open pool by cooperating with other miners [6]. Many miners spend plenty of computing power on creating a block. In other words, producing block is to solve a complex problem, or to generate a full poof of work. Miners get the corresponding payoff through sending poof of work to the pool, while they might as well send partial proof of work to the open pool since a full pool of work is difficulty to be discovered. Moreover, this pool allocates equality according to the contributed power ratio in whole system. However, a miner can sabotage an open pool by seemingly joining it but never sharing its power. The attacker only sends a partial proof of work to pool, and discards the full proof of work when it is discovered. This situation is called block withholding attack [7]. In an open pool, miners choose either to attack or cooperate with other miners to gain its own payoff. When all miners attack each other, they earn less than that they would have if none had attacked, that is the mining dilemma [8-9] in PoW consensus process, this dilemma also corresponds to the famous of Prisoner's Dilemma in the game theory [10], namely, it is the optimal choice for individual to attack, but not the best for system. Similarly, for all miners mine in an open pool, whether or not attack is a miner's dilemma, attack is the best choose for one miner, while attack will make the system obtain a low welfare. With the purpose that promoting miners cooperatively mine in pool, to get a high social revenue, it is necessary to develop or optimize the incentive mechanisms to promote cooperative mine in PoW consensus algorithm in blockchain [11-13].

PoW consensus mechanism aims at ensuring the consistency of bitcoin distributed accounting system. Unfortunately, it also holds many shortcomings. There are some improved consensus algorithms, such as Proof of Stake (PoS) [14], which changes the power of the PoW into the system rights, greater ownership of player has greater probability of becoming the next to account. PoS is both energy saving and time saving, while it is prone to fork, and also needed to mine. Delegated Proof of Stake (DPoS) [15] depending on PoS plays the role of accounting professionals, in which the accounts are kept by the player selected by the rights. It significantly reduces the number of nodes involved in authentication and accounting, and reaches the second

[*]This work is supported by the National Natural Science Foundation of China under Grant 61272007, 61503342, and the Natural Science Foundation of Zhejiang Province under Grant LY16F030002 and Q13F020029.

level of consensus verification. Whereas it still relies on tokens. The Verified Pool [16] based on the traditional distribution consensus technology uses data verification mechanism. It works without tokens, keeping a low degree of decentration. The Delegated Byzantine Fault Tolerance algorithm [17] selects bookkeepers selected by the rights to achieve a consensus, which maximizes the integrity of the system but also forks a lot. None of the present consensus mechanisms is perfect or apt to all the application scenarios. Lewenberg Y et. al. [18] propose an alternative structure to the chain for higher rates, and analyzes the security protocol to decrease the attacks between miners. Moreover, a new protocol that just uses cryptography principle without generating cryptogram is proposed to guarantee the transactional privacy [19]. A new method that weights tuning laws in critic neural networks to achieve a Nash Equilibrium to assure the system stability is presented in [20]. Optimal control scheme methods are also proposed for nonlinear systems, for example, the iterative two-stage dual heuristic programming [21] or the adaptive dynamic programming [22], are based on the change of system state.

In order to prevent participants from being trapped in a prisoner's dilemma [23-24], the ZD strategy [25-26] is employed as a probabilistic and conditional strategy in the iterated game to cope with the "*free-riding*" problem. With the ZD strategies, the player is able to unilaterally set the expected utility of an opponent or a ratio of the player's expected payoff to its opponent's, whatever the opponent's strategy is.

The zero-determinant (ZD) strategy is applied in many fields. It is used in wireless communication for cooperation of resource sharing in many works [27-30]. In [31], the ZD strategy is applied in iterated public goods game, while in [32], Ashraf et al. model the secondary sharing of wireless spectrum as an iterated game, and a ZD strategy is used to control the outcome of opponents in a certain range or to achieve any feasible outcome.

To avoid a low social welfare since miners attack each other, we consider a LM, a loyal miner who cares about the whole pool revenue, and a SM, a selfish miner who only concerns about its own payoff and manages to get high reward, and take the mining as an iterated game. At each game iteration, both the LM and the SM choose to cooperate or to attack. Derived from the original ZD strategies proposed by Press and Dyson [24], we put forward a subclass ZD strategy, a pinning strategy, for the LM, to control the payoff of SM unilaterally at a threshold value, and ultimately to increase the welfare of society, no matter what the strategy of SM is.

The rest of this paper is organized as followings: Section 2 analyzes the miner's dilemma in an open pool, and builds system model. In Section 3, we propose a pinning strategy to optimize the mining model in the PoW consensus process, then the game analysis is given. Numerical simulation's analysis and results are presented in Section 4. Finally, we give the conclusion in Section 5.

2 System Model

In an open pool, when a loyal miner sends a full or partial proof of work to the pool, he will be allocated with a fair reward depending on its contributed power. Unfortunately, some miners may not work faithfully, they launch a classical block withholding attack, by just sending partial proof of work, and abandoning the full proof of work whenever it is found. In addition, the attacked pool will divide its welfare equally among all the attackers, therefore each miner, containing the attackers certainly, earns less because the attackers will get less than that they do not attack. However, in some cases, attackers will gain higher payoff than the price they paid, that is the "*free riding*" theory in mining.

The LMs mine regularly with their power consumed. The cooperation in an open pool increases the probability of block generating, and also expands the expected payoff. Miners in an open pool will face a prisoners' dilemma. Suppose that the power consuming is c, the enlarging multiples of payoff is r (r>1), r (1-c)>1/2, and c>1/2. We consider there are two miners mining in pool, LM and SM, each miner has two strategies: cooperation (C) and attack (A), when regularly mine, the two miners' payoffs are 1 and the payoff in different strategies is expressed as:

LM SM	C	A
C	r/2-c r/2-c	1/2-c 1/2
A	1/2 1/2-c	0 0

In the open pool, the interaction between LM and SM is regarded as an iterative game. At each iteration, we model the mining between the LM and SM as a single stage of prisoner's dilemma game. When the combination of their strategies is (C, C), the payoff of LM and SM are R^L_R, R^S_R respectively. When the strategy combination is (C, A), the payoffs are R^L_S, R^S_T. Given the combination of (A, C), the payoffs are R^L_T, R^S_S, and when (A, A), the payoffs are R^L_P, R^S_P, respectively. With the payoff matrix, $R^L_R = r/2\text{-}c$, $R^S_R = r/2\text{-}c$, $R^L_S = 1/2\text{-}c$, $R^S_T = 1/2$, $R^L_T = 1/2$, $R^S_S = 1/2\text{-}c$, $R^L_P = 0$, $R^S_P = 0$.

In the iterated game, it is proved that the long-memory player has no advantage over the short-memory player when each stage game is iterated identically infinite times [24]. Hence, we suppose the two miners have memory of only one single previous move, in other words, at current iteration of the game, the actions of both miners only depend on the payoffs of the previous round. When take an iterated process of game into account, both LM's and SM's mixed strategies are supposed as p = [p_1, p_2, p_3, p_4] and q = [q_1, q_2, q_3, q_4] for their probabilities of cooperation based on the previous iteration, cooperation or attacking strategies. Namely, p and q represent the transition probability vectors for the cooperation state in the next state. When the two miners adopted cooperation in the previous stage, and the LM chooses cooperation at present, the conditional probability of LM is p_1, and the conditional probability for SM to choose cooperation strategy is q_1. When both the LM and the SM choose to attack, their conditional probabilities are (1-p_1) and (1-q_1) respectively. Similarly, when the LM and the SM choose different strategies in the previous stage, the conditional probability for LM and SM to take cooperation strategy is shown in fig. 1 and fig. 2.

In the following section, we consider the case where two miners mine in an open pool, one miner is a LM, the other is a SM. The pinning strategy for the LM, a subclass of the ZD strategy, is proposed to promote SM to mine cooperatively,

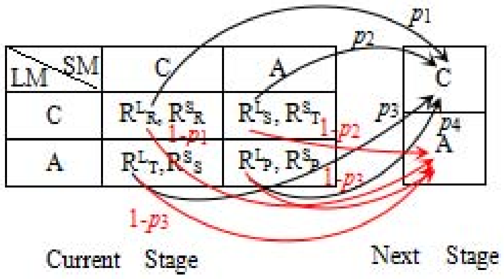

Fig. 1. The conditional strategy of LM

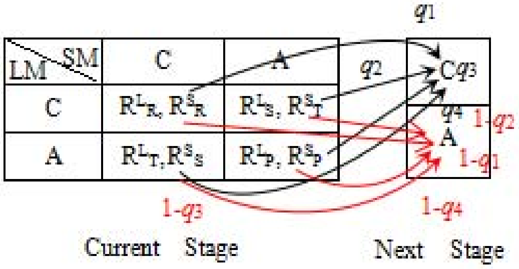

Fig. 2. The conditional strategy of SM

so as to set the payoff of SM and then to reach a relatively high stable social revenue unilaterally.

3 Game Analysis

Following the above game model, we define X, Y to represent the LM's and SM's actions, X∈[C, A], Y∈[C, A]. Under the initial conditions, the procedure of the repeated game is a stochastic process. Label the payoffs of the previous strategy as 1, 2, 3 and 4, with the payoff XY∈[CC, CA, AC, AA]. With the payoff matrix, the payoff vector of LM in four different states is $R^L=[R^L_R, R^L_S, R^L_T, R^L_P]^T=[r/2-c, 1/2-c, 1/2, 0]^T$, and that of the SM is $R^S=[R^S_R, R^S_T, R^S_S, R^S_P]^T=[r/2-c, 1/2, 1/2-c, 0]^T$.

An iterated game can be represented with the Markov process, and the state transition of Markov process is completely determined by p and q, hence the Markov transition matrix M(p, q) is defined as

$$\mathbf{M}=\begin{bmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (4-p_4)(1-c_4) \end{bmatrix} \quad (1)$$

Define the stationary vector of Markov matrix M as $v = [v_1, v_2, v_3, v_4]^T$, where v_1, v_2, v_3 and v_4 are the four different states of probabilities, (C, C), (C, A), (A, C), (A, A), and $v_1 + v_2 + v_3 + v_4=1$. Since M has a unit eigenvalue, denote $\mathbf{M}'=\mathbf{M}-\mathbf{I}$, where $\mathbf{I}$ is a unit matrix, and $\mathbf{M}'$ is a singular matrix. We have

$$\mathbf{v}^T\mathbf{M}=\mathbf{v}^T,\ \mathbf{v}^T\mathbf{M}'=0. \quad (2)$$

According to the Cramer's ruler, the $\mathbf{M}'$ and its adjugate matrix adj($\mathbf{M}'$) meet

$$\mathrm{adj}(\mathbf{M}')\mathbf{M}'=\det(\mathbf{M}')\mathbf{I}=0 \quad (3)$$

Following equation (2) and (3), v is proportional to every row of $\mathrm{adj}(\mathbf{M}')$. With the Laplace expansion rule, $\det(\mathbf{M}')$ is equal to the last row of $\mathrm{adj}(\mathbf{M}')$ dot product the last column of $\mathbf{M}'$, and the last column is replaced by an arbitrary four vector $f=[f_1, f_2, f_3, f_4]^T$, so that

$$\mathbf{v}\cdot\mathbf{f}\equiv D(p,q,\mathrm{f})$$

$$=\det\begin{bmatrix} -1+p_1q_1 & -1+p_1 & -1+q_1 & f_1 \\ p_2q_3 & -1+p_2 & q_3 & f_2 \\ p_3q_2 & p_3 & -1+q_2 & f_3 \\ p_4q_4 & p_4 & q_4 & f_4 \end{bmatrix} \quad (4)$$

In equation (4), the second column of D(p, q, f) is controlled only by LM, While the third column of D(p, q, f) is controlled by SM, define

$$\begin{aligned} \mathrm{p}'&=[-1+p_1,-1+p_2,p_3,p_4] \\ \mathrm{q}'&=[-1+q_1,q_3,-1+q_2,q_4] \end{aligned} \quad (5)$$

When f = R^L, the expected payoff of LM in the stationary state is

$$\mathrm{U}^L=\frac{\mathrm{v}^T\cdot \mathrm{R}^L}{\mathrm{v}\cdot 1}=\frac{D(p,q,\mathrm{R}^L)}{D(p,q,1)} \quad (6)$$

When f=R^S, the expected payoff of the SM in the stationary state is

$$\mathrm{U}^S=\frac{\mathrm{v}^T\cdot \mathrm{R}^S}{\mathrm{v}\cdot 1}=\frac{D(p,q,\mathrm{R}^S)}{D(p,q,1)} \quad (7)$$

Where the denominator D(p,q,1) is used to normalize the payoffs. Given f=$\alpha R^L+\beta R^S+\gamma 1$, D(p, q, f) is a singular matrix, and the linear combination of the payoff vectors R^L and R^S meet

$$\alpha\mathrm{U}^L+\beta\mathrm{U}^S+\gamma=\frac{D(p,q,\alpha\mathrm{R}^L+\beta\mathrm{R}^S+\gamma)}{D(p,q,1)} \quad (8)$$

where α, β, γ are non-zero parameters.

When the LM takes strategies of αR^L, βR^S, or a linear combination of them, he will have the possibility of choosing unilateral strategies to make the determinant in numerator vanish. Similarly, the same about SM. e.i., if the LM adopts a strategy which satisfies p=$\alpha R^L+\beta R^S+\gamma 1$, or the SM takes a strategy with q=$\alpha R^L+\beta R^S+\gamma 1$, then the determinant vanishes. Accordingly, between the LM and the SM expected payoffs will be satisfied a linear relationship

$$\alpha\mathrm{U}^L+\beta\mathrm{U}^S+\gamma=0 \quad (9)$$

When the parameters α and β have different value, we have different subclass of ZD strategies.

The pinning strategy is one of the subclass of ZD strategy, in which a miner could control the payoff of another miner, no matter what strategy the other miner takes. Taking a pinning strategy with α=0, a LM can determine the payoff of its opponent, namely p=$\beta R^S+\gamma 1$. Set f=$\beta R^S+\gamma 1$, then equation (8) becomes

$$\beta\mathrm{U}^S+\gamma=\frac{D(\beta\mathrm{R}^S+\gamma 1,\mathrm{q},\beta\mathrm{R}^S+\gamma 1)}{D(\beta\mathrm{R}^S+\gamma 1,\mathrm{q},1)}=0$$

That is to say, as long as the LM applies a pinning strategy, the payoff of the SM will be set by β and γ, namely, U^S= -γ/β.

Following the strategy p=$\beta R^S+\gamma 1$, get p_2, p_3, β and γ by solving the four equations with fixed p_1 and p_4

$$p_2=\frac{p_1-(1+p_4)(1-r+2c)}{r-2c} \quad (10)$$

$$p_3=\frac{(2c-1)(1-p_1)+p_4(r-1)}{1-2c} \quad (11)$$

$$\beta=\frac{-2+2p_1-2p_4}{r-2c}$$

$$\gamma = p_4$$

Then,

$$\mathrm{U^S} = \frac{p_4(r-2c)}{2\text{-}2p_1 + 2p_4} \tag{12}$$

$$\mathrm{U^L} = \frac{(r-2c)[p_4(r-1)+2c(1-p_1)]}{2(r-1)(1-p_1+p_4)} \tag{13}$$

In equation (10) and (11), when p_1 and p_4 approaches 1 and 0 respectively, p_2 tends to 1 from 0 while p_3 draws near to 0 from 1. In equation (12) and (13), when p_1 gets gradually close to 1, regardless of the value of p_4, the payoff of the SM approaches (r/2-c), the payoff of the LM also gets closer to (r/2-c). The payoff of the SM converges to 0 when p_4 approaches to 0 no matter what the value of p_1 is. However, the LM's payoff is $c(r\text{-}2c)/(r\text{-}1)$ not 0. That is, LM can set the payoff of the SM into a range, from mutual cooperation to mutual attack, no matter what strategies the SM takes, while its own payoff changes along with the strategy it chooses.

With the pinning strategy, the LM also tries to control its own payoff by setting p=$\alpha\mathrm{R^L}+\gamma 1$ and $\alpha\mathrm{U^L}+\gamma$=0. We pin p_1 and p_4 yet, p_2 and p_3 can be solved as,

$$p_2 = \frac{(1+p_4)(r-1)-p_1(2c-1)}{r-2c}$$

$$p_3 = \frac{p_1 - 1 - p_4(1-r+2c)}{r-2c}$$

p_2 and p_3 are conditional probabilities, and $0 \le p_2 \le 1$, $0 \le p_3 \le 1$. Given the conditional probabilities of LM, p_1=1, p_2=1, p_3=0, p_4=0, the conditional probability vector of LM is p=[1, 1, 0, 0], which means that if LM took a cooperation strategy at previous stage, it will choose to continue cooperation at this stage. Analogously, it tends to choose to attack other miners at the present stage if he did attack others at the previous stage. In short, if the LM always chose to cooperate or attack, it can't control himself payoff unilaterally.

Theorem 1: When LM takes a pinning strategy, it can unilaterally set the payoff of SM within a range from 0 to r/2-c, regardless of the SM's strategy. The SM's payoff is proportional to r but inversely proportional to c. while the LM can't control its own payoff even with any subclass of ZD strategy.

4 Simulation Results

In this section, different scenarios are illustrated to appraise the performance of the proposed pinning strategies in the iterated mining dilemma. In the first three scenarios as shown in Fig.3, LM takes the pinning strategy, the WSFS strategy (namely, p=[1, 0, 0, 1]), and the TFT strategy (namely, p=[1, 0, 1, 0]), respectively, while the SM adopts the WSFS strategy all the time. In the following three cases shown in Fig.4, the LM uses the pinning strategy, the WSFS strategy, and the TFT strategy, respectively, while the SM takes the TFT strategy all along. In the rest four cases (Fig.5), the LM also takes the four different strategies while the SM adopts different strategies, q=[0.1, 0.2, 0.3, 0.4], respectively. Without losing generality, set α=0, β=-8, the factor expand multiples of payoff r=2, and consume of outcome c=2/3. The revenue vectors of the LM and SM in four states are $\mathrm{R^L}$=[1/3, -1/6, 1/2, 0]$^\mathrm{T}$ and $\mathrm{R^S}$=[1/3, 1/2, -1/6, 0]$^\mathrm{T}$, respectively.

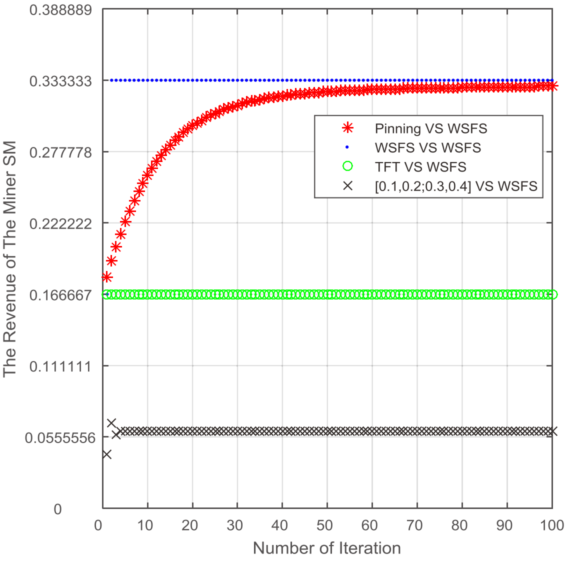

Fig. 3. The LM takes different strategy and the SM adopts the WSFS strategy

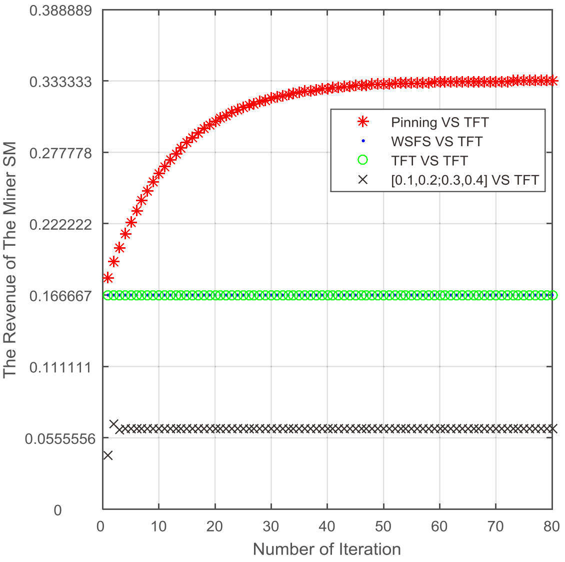

Fig. 4. The LM takes different strategy and the SM adopts the TFT strategy.

In Fig. 3, the SM always takes a WSFS strategy, while the LM takes the pining strategy, and the payoff of SM is kept to a specific value 1/3, which means that the LM can either set the payoff of SM or control the SM to choose to cooperate with the LM through a pinning strategy. When the LM takes a WSFS strategy, the payoff of the SM is pinned at a fixed value. While the LM adopts a TFT strategy, the payoff of SM is fixed as 1/6, which isn't the maximum value. When the LM applies [0.1, 0.2, 0.3, 0.4] strategy, the payoff of the SM is pinned at a relatively low value. Therefore, when SM takes a WSFS strategy, the best strategy for LM is the pinning strategy or the WSFS strategy, while the worst is [0.1, 0.2, 0.3, 0.4].

In Fig.4, the SM implements a TFT strategy and the LM adopts a pinning strategy. The welfare of the SM is fixed at a certain value, and both miners mine cooperatively. When the LM takes a WSFS strategy or a TFT strategy, the payoff of the SM is lower than that in the case that they cooperate with

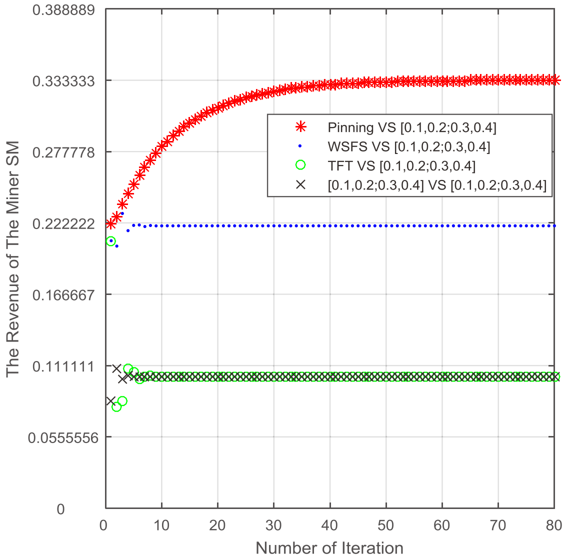

Fig. 5. The LM takes different strategies and the SM adopts the strategy [0.1, 0.2, 0.3, 0.4].

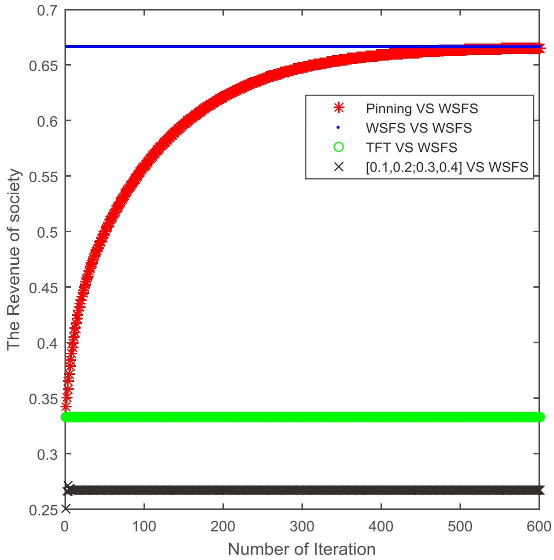

Fig. 6: The LM takes different strategies and the SM adopts the WSFS strategy.

each other. When the LM applies the strategy of [0.1, 0.2, 0.3, 0.4], the payoff of the SM gets a low value. In short, when SM takes a TFT strategy, the best choice for the LM is the pinning strategy, and the worst is [0.1, 0.2, 0.3, 0.4].

In Fig. 5, the LM takes the pinning strategy, and the SM cooperates with the LM gradually to improve its payoff When the LM takes a WSFS strategy, the payoff of SM gets reduced. If the LM applies a TFT strategy or the [0.1, 0.2, 0.3, 0.4] strategy, SM will be rewarded with the lowest value.

As for the first situation shown in Fig. 3-5, as long as the LM takes the pinning strategy during mining, it could set the payoff of the SM approach gradually to 1/3, e.i., the LM could control SM to select a cooperative strategy after a certain number of iterations.

In Fig. 6, when the SM takes a WSFS strategy and the LM adopts the pinning strategy or a WSFS strategy, the revenue

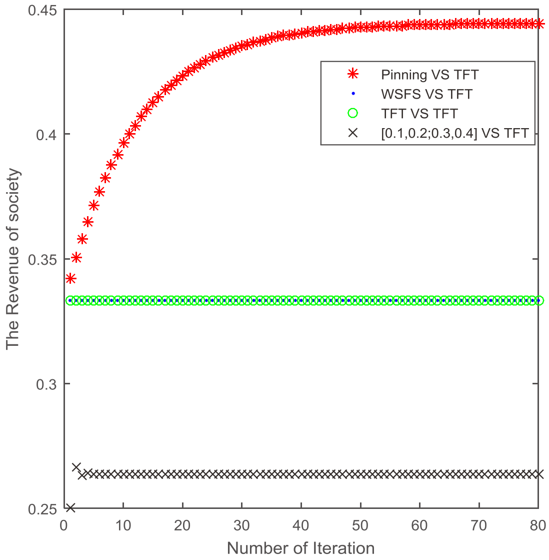

Fig. 7. The LM takes different strategies and the SM adopts theTFT strategy.

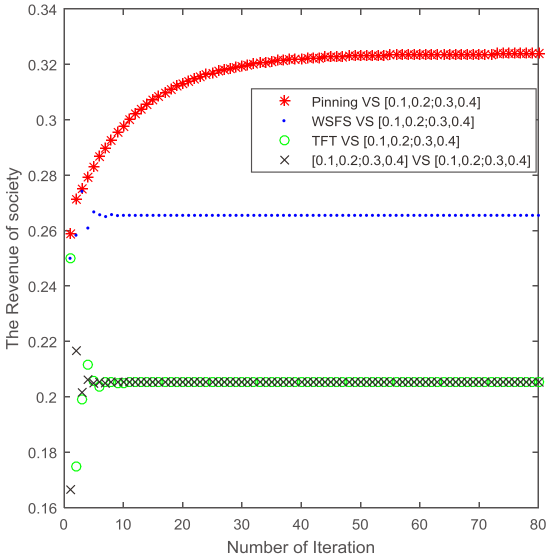

Fig. 8. The LM takes different strategies and the SM adopts the strategy of [0.1, 0.2, 0.3, 0.4].

of the society could achieve a high value, where both of the miners choose to cooperate in mining. Once the LM takes TFT strategy or [0.1, 0.2, 0.3, 0.4] strategy, the revenue of society couldn't be satisfied. When the SM applies a WSFS strategy, the best choice for the LM is to take a pinning or WSFS strategy, while the worst strategy is [0.1, 0.2, 0.3, 0.4].

In Fig. 7 where the LM adopts a pinning strategy, the society's revenue reaches a relatively high value. When the LM applies a WSFS or TFT strategy, the system gets lower benefits. When the LM takes [0.1, 0.2, 0.3, 0.4], the society's revenue is the lowest.

In Fig. 8, when LM applies a pinning strategy, the society's revenue can be satisfied. When LM applies WSFS, the system gets the lower benefits. When LM takes TFT strategy or [0.1, 0.2, 0.3, 0.4], the society's revenue falls to the lowest point.

As shown in Fig.6-8, the LM just takes a pinning strategy in mining, regardless of the strategy that the SM takes, the society revenue reaches a relative high value. Especially, when the SM takes a WSFS strategy, too, the revenue of society gets the highest value. In such a way, the LM can set society's revenue after a certain number of iterations, no matter what the SM's strategy is.

5 Conclusion

In this paper, we analyze the miners' dilemma in the PoW consensus process, and optimize the PoW consensus through game theory. To prevent the two miners to attack each other, we propose a pinning strategy, a subclass of ZD strategy, which can set the payoff of SM and therefore improve the social revenue Simulation results confirm that when the LM takes a pinning strategy, the bitcoin system obtains relative higher social revenue, regardless of the SM's strategy. Besides, we have proved that the LM can't control its own payoff with any strategy.

Based on the analysis of the pinning strategy, we find that the payoff of SM is proportional to r but inversely proportional to c. Hence, to improve the probability of the SM's cooperation and increase the revenue of society, the blockchain system can be optimized by improving the value of r or reducing the value of c, or applying a pinning strategy.

References

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

[2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 2009.

[3] Block chain depth report: the world be your witness(2). http://www.wxrw123.com/rm/20160420/472846_2.html, April 20, 2016.

[4] McConaghy T, Marques R, Müller A, De D J, McConaghy T, McMullen G, et al. BigchainDB: A Scalable Blockchain Database. https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf, June 8, 2016.

[5] Blockchain introduction. http://blockchaindev.org/article/introduce_blockchain.html, December 14, 2015.

[6] Consensus in Bitcoin: One system, many models. https://freedom-to-tinker.com/blog/randomwalker/consensus-in-bitcoin-one-system-many-models/, December 26, 2014.

[7] Nicolas T C. Bitcoin Miner Optimization. https://www.knaw.nl/shared/resources/actueel/bestanden/140212_Bitcoin_presentatie_Nicolas_Courtois.pdf, 2013

[8] Eyal I. The Miner's Dilemma. *Computer Science*, 89-103, 2014.

[9] Study when be threatened, the bitcoin pool attacking. http://www.bitecoin.com/online/2015/01/11102.html, January 4, 2015.

[10] Tang C B, Li A, and Li X. When reputation enforces evolutionary cooperation in unreliable MANETs. *IEEE Trans. Cybern*, 45(10): 2190-2201, 2015.

[11] E yal I, Gün E S. It's Time For a Hard Bitcoin Fork. http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/, June 3, 2014.

[12] Rosenfeld M. Analysis of Bitcoin Pooled Mining Reward Systems. *Computer Science*, 2011.

[13] Courtois N T, Bahack L. On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency. *Eprint Arxiv*, 2014.

[14] Larimer D. Transactions as proof-of-stake. http://7fvhfe.com1.z0.glb.clouddn.com/@/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf, 2013.

[15] Larimer D. Delegated proof-of-stake white paper. http://www.bts.hk/dpos-baipishu.html, 2014.

[16] The consensus mechanism in blockchain. http://blog.csdn.net/u013137970/article/details/52958176, October 28, 2016.

[17] Zhang Zhengwen. A Byzantine Fault tolerant algorithm in blockchain. http://www. onchain.com/paper/66c6773b.pdf, April, 2016.

[18] Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive block chain protocols//International Conference on Financial Cryptography and Data Security. *Springer Berlin Heidelberg*, 2015: 528-547.

[19] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *IEEE Symposium on Security and Privacy*, 839-858, 2016.

[20] Zhang H, Cui L, Luo Y. Near-Optimal Control for Nonzero-Sum Differential Games of Continuous-Time Nonlinear Systems Using Single-Network ADP. *IEEE Transactions on Systems Man & Cybernetics Part B Cybernetics A Publication of the IEEE Systems Man & Cybernetics Society*, 43(1):206-216, 2013.

[21] Zhang H, Qin C, Luo Y. Neural-Network-Based Constrained Optimal Control Scheme for Discrete-Time Switched Nonlinear System Using Dual Heuristic Programming. *IEEE Transactions on Automation Science & Engineering*, 11(3):839-849, 2014.

[22] Zhang H, Cui L, Zhang X, et al. Data-Driven Robust Approximate Optimal Tracking Control for Unknown General Nonlinear Systems Using Adaptive Dynamic Programming Method. *IEEE Transactions on Neural Networks*, 22(12):2226-2236, 2011.

[23] Block Withholding Attacks-Recent Research. http://blog.bettercrypto.com/?p=1131, December 2, 2014.

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

[25] Dong, Rong, Zhi-Hai, and Zhou T. Zero-determinant strategy: An underway revolution in game theory. *Chinese Physics B*, 23(7):164-170, 2014.

[26] He X, Dai H, Ning P, et al. Zero-determinant Strategies for Multi-player Multi-action Iterated Games. *IEEE Signal Processing Letters*, 23(3):311-315, 2016.

[27] Zhang H, Niyato D, Song L, Jiang T, Han Z. Zero-Determinant Strategy for Resource Sharing in Wireless Cooperations. *IEEE Transactions on Wireless Communications*, 15(3): 2179-2192, 2016.

[28] Zhang H, Dusit N, Song L, et al. Zero-determinant strategy in cheating management of wireless cooperation. I*EEE GLOBECOM*, 4382-4386, 2014.

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

[30] Nash J F. Equilibrium Points in N-Person Games. *Proceedings of the National Academy of Sciences of the United States of America*, 36(1): 48-49, 1950.

[31] Pan L, Hao D, Rong Z, Zhou T. Zero-determinant strategies in iterated public goods game. *Scientific Reports*, 13096-13096, 2014.

[32] Ashraf Al D, George K, Jorg L. Zero-Determinant Strategies: A Game-Theoretic Approach for Shring Licensed Spectrum Bands. *IEEE Journal on Selected Areas in Communications*, 32(11): 2297-2308, 201