Journal of Systems Science and Information
Jun., 2021, Vol. 9, No. 3, pp. 266–279
DOI: 10.21078/JSSI-2021-266-14

The Evolutionary Equilibrium of Block Withholding Attack

Yukun CHENG*
School of Business, Suzhou University of Science and Technology, Suzhou 215009*, China*
E-mail: *ykcheng@amss.ac.cn*

Zhiqi XU
School of Business, Suzhou University of Science and Technology, Suzhou 215009*, China*
E-mail: *joisexzq*@163.*com*

Shuangliang YAO
Jiangsu University of Science and Technology, Zhenjiang 212008*, China*
E-mail: *justysl@just.edu.cn*

Abstract Bitcoin is the most famous and the most used cryptocurrency in the world, such that it has received extreme popularity in recent years. However the Bitcoin system is accompanied by different attacks, including the block withholding (BWH) attack. When a miner plays the BWH attack, it will withhold all the blocks newly discovered in the attack pool, damaging the honest miners' right to obtain the fair reward. In this paper, we consider a setting in which two miners may honestly mine or perform the BWH attack in a mining pool. Different strategy profiles will bring different payoffs, in addition influence the selection of the strategies. Therefore, we establish an evolutionary game model to study the behavior tendency of the miners and the evolutionary stable strategies under different conditions, by formulating the replicator dynamic equations. Through numerical simulations, we further verify the theoretical results on evolutionary stable solutions and discuss the impact of the factors on miners' strategic choice. Based on these simulation results, we also make some recommendations for the manager and the miners to mitigate the BWH attack and to promote the cooperation between miners in a mining pool.

Keywords block withholding attack; blockchain; Bitcoin; evolutionary game; evolutionary stable strategies

1 Introduction

Bitcoin is a cryptocurrency, originally proposed by Nakamoto[1]. Unlike the existing currencies, Bitcoin is decentralized and runs without administrators. Because of this, it has become a great success. One of the key technologies which Bitcoin relies on is the blockchain. Blockchain is a public distributed ledger in which all the network nodes can participate to verify the transactions. Such a structure is beneficial to keep the data integrity, continuity, and consistency,

Received August 25, 2020, accepted January 18, 2021
Supported by the National Nature Science Foundation of China (11871366), Qing Lan Project for Young Academic Leaders, Qing Lan Project for Key Teachers, and the Research Innovation Program for College Graduate Students of Jiangsu Province (KYCX20-2790)
*Corresponding author

which makes the blockchain possess several nice features, such as decentralization, programmability and security.

As one of the most successful applications of blockchain technology, Bitcoin system leverages the consensus protocal of Proof-of-work (PoW) to maintain the properties of consistency and security of data[2]. To reach an agreement among all nodes, PoW requires the participants to solve a complex SHA 256 mathematical puzzle, which is hard to calculate but easy to be verified[3], by consuming their computational power. The one who first solves the puzzle is the winner and it has the right to broadcast its verified block to the blockchain network and then obtains the corresponding reward. Generally, these participants who calculate the puzzle are named as miners, and the process to solve puzzle and obtain the reward is called mining.

To obtain the reward from the Bitcoin system, all miners compete to be the first to solve the puzzle and generate the block. Generally, the system automatically adjusts the difficulty of the block generation, to maintain the average time interval to create a block about 10 minutes. Because of the increased difficulty of the system and the small computational power, a solo miner rarely generates a block. Although the expected revenue of a miner is positive, a miner has to wait for a quite long time to create a block and to earn the actual reward. Therefore, joining a mining pool is a good choice for a solo miner. Generally, a mining pool consists of a pool manager and a group of miners. The main task of the manager is to outsource the work to the miners. Once a miner submits a full proof of work (FPoW) to the manager, then the manager will send this FPoW to the Bitcoin system. When the manager receives the full revenue of the block from the system, it shall fairly allocate this revenue to the miners according their computational power. At the same time, the mining pool also accepts the partial proof of work (PPoW) and estimates the miner's computational contribution according to the rate with which it submits this PPoW. Such contribution is an important evidence for the manager to distribute the revenue to these miners who only submit PPoW.

Due to the opening pool, the Bitcoin system faces several kinds of attacks, such as selfish mining attacks[4], FAW attacks[5], block withholding (BWH) attacks[6] and DDOS attacks[7]. In this paper, we mainly focus on the BWH attacks. When a miner plays the BWH attack, it only sends the PPoW to the manager and discards the FPoW. On the one hand, since the attacker discards every FPoW, it does not bring any contributions to the pool. On the other hand, the attacker can share the revenue obtained by other miners, as it submits a PPoW to the pool. Obviously, the BWH attack seriously damages the honest miners' right to obtain the fair reward.

In this work, we will discuss the BWH attack in a mining pool by constructing an evolutionary game model. To simplify our evolutionary game model, suppose there are two miners in a pool, each of whom has two strategies. One is to cooperate, i.e., mine honestly, and the other is to launch the BWH attack. In each round of the evolutionary game, both of miners observe each other's strategy, and adjust their current low income strategies to the higher income strategies. We are more interested in the evolutionary stable strategies (ESS) of the game and how different factors prompt the cooperation tendency between miners.

1.1 Related Work

When a miner plays the BWH attack in a mining pool, it only submits PPoW and discards FPoW, which makes the manager be convinced that this attacker is indeed trying to mine for the pool. Because the manager mistakes the attacker as an honest miner, it also allocate revenue among the attacker and other pool miners. The BWH attack was first proposed by [8]. In 2014, a mining pool called Eligius suffered the BWH attack and lost 300 BTC[9]. Since then, different kinds of research have paid attention to this attack.

Eyal[6] first applied a pool game between two mining pools to analyze the Nash equilibrium of the BWH attack. In the case of [6], two pools shall make decisions whether or not attack, which is similar to the famous Prisoners' Dilemma and thus is called Miner's Dilemma. In order to prevent the pools from being trapped in a miner's dilemma and to optimize the mining model, [3] proposed a subclass Zero Determinant (ZD) strategy, by which a miner could control another miner's payoff and increased the social revenue. [10] modeled a computational power splitting game and showed that the attacker can gain profits in the long-run and may not be so for a short time, implying that the existing pool reward sharing protocols in Bitcoin are insecure when the miners launch the BWH attack.

By deepening of study on the BWH attacks, more researchers pay attention to the mitigation strategies of the BWH attack. [2] believed that most of the countermeasures to mitigate the BWH attack change the mining algorithm, which lowers the practical adaptability. So, the authors suggested three necessary conditions for the BWH countermeasure: No loss, compatibility, and fairness. The incentive compatibility of the reward allocation mechanisms of mining pool was introduced by [11], which can encourage the miners to submit blocks immediately and guarantee the mining pool's revenue. A concept called *"special reward"* was proposed by [12], granting additional incentive to the miner who submits a valid block to the pool and the BWH attacker would never receive the special reward. In this scheme, the revenue that the attacker gains is less than his expectation and thus could make a mining pool repulse the BWH attackers. [13] presented two schemes to counter the BWH attack, the one applies the cryptographic commitment schemes and the other is an alternative implementation by using hash function, both making it impossible for miners to distinguish between full proof of work and partial proof of work. A generalized model was constructed by [14] to analyze the equilibrium of the BWH attack, in which the authors found that increasing the asymmetry of information by information conceal mechanisms could decrease the negative influence of the BWH attack on the pool.

In decision-making research, evolutionary game theory is a common tool for constructing a model and analyzing the choice of strategies[15]. Classic game theory assumes that all players have perfect rationality, while evolutionary game theory is only based on the bounded rationality[16]. That is, the choice of each player's equilibrium strategy is the result of the continuous learning and adjustment, rather than a one-time choice. The basic solution concept of the evolutionary game theory is evolutionary stable strategy (ESS)[17], and it is used to describe the stable state of the evolution process. Recently, a few kinds of literatures study on the blockchain by using evolutionary game theory. [18] applied the evolutionary game to describe the dynamic mining-pool selection process in a PoW-based blockchain network, and

they provided the theoretical analysis of the evolutionary stability under the two-pool condition. [19] modeled the process of mining as a two-stage game model in order to characterize the decision that the pool whether to open or not and to launch the BWH attack or not in the PoW-based blockchain network. They applied the evolutionary game theory and analyzed evolutionary stability of the strategy selection. This method could overcome the shortcoming of the NE which only describes the local optimization of the pool strategies selection. In [20], the authors investigated the evolutionary mining game with miner's dilemma under the BWH attack and studied the population changes with the time between participated pools through the evolutionary stability. They also analyzed the mining pool dynamics affected by malicious infiltrators and the feasibility of autonomous migration among individual miners.

Few work studies the BWH attacks by the evolutionary game from the perspective of mitigating the attacks. [21] constructed a symmetrical evolutionary game model to analyze the expected benefits of the strategy selection of two miners in a mining pool, where the computational power of the two miners are the same. The authors explored how the pool administrator could mitigate the BWH attack under different supervision and punishment mechanisms. In this paper, an asymmetric evolutionary game model, more general than the symmetrical one, is constructed, in which there are two miners in a mining pool and they have different amounts of computational power. Our objects are to explore the influence of the main factors on the miners' strategy selections, and to make suggestions to mitigate the BWH attack to promot the cooperation between miners.

1.2 Paper Organization

In this paper, we analyze the BWH attack in a pool by establishing an evolutionary game model. Motivated by [14], we construct the payoff functions under different strategies in Section 2. By establishing the replicator dynamic equations, different evolutionary stable strategies under different conditions are derived in Section 2. In Section 3, we analyze how different factors influence the miners' strategic choice by a series of simulations. Last section provides several valuable suggestions and concludes this paper.

2 The Evolutionary Game Model for the BWH Attack

In this section, we first establish an evolutionary game model to study the BWH attack in a Bitcoin mining pool, and analyze the evolutionary stable strategies by using the replicator dynamic equations.

2.1 Basic Evolutionary Game Model

Generally, there are many miners in a Bitcoin mining pool. Since this work only concentrates on two strategies: One is honestly mining (C) and the other is the BWH attack (A), let us assume that there are two participants: Miner 1 and miner 2 to simplify our discussion, like [3, 22], each of whom has aforementioned two strategies. Therefore, we construct an evolutionary game model, in which there are four strategy profiles: (C, C), (C, A), (A, C) and (A, A). Different strategy profile would bring different payoffs to each miner. During the evolutionary game, the miners keep learning to adjust their low-income strategies and to imitate the strategy choice of the miner, who has a higher income, until the strategy profile of two miners

reaches a stable state. To establish the evolutionary game model between two miners formally, following assumptions and parameters are necessary to be introduced in advance, which are similar to those in [14].

1) Two miners own different amounts of computational power. Let miner 1 and miner 2 have a_1 and a_2 units of computational power, respectively. W.l.o.g, we assume that $a_2 = \lambda a_1$, where $\lambda \in [0, 1]$.

2) The reward the mining pool obtains per unit computational power per unit time is denoted by R.

3) When the miner honestly mines and sends the full proof of work (FPoW) to the manager instantaneously, the cost of computational power per unit time to mine is C_1 ($C_1 > 0$). If the miner employs the BWH attack to only submit the partial proof of work (PPoW), the mining cost per unit time it consumes is C_2 ($0 \leq C_2 < C_1$).

4) If both of the two miners honestly mine, then the probability to dig up the legal block will increase, which leads to the improvement of the expected profit. Thus we assume that the miners' cooperation with each other would enlarge γ multiples of reward ($\gamma > 1$).

5) To encourage the miners to cooperate, the pool manager will draw an additional reward from the reward R to offer to the one who submits the FPoW. We assume the additional reward per unit computational power per unit time to be δR, where $\delta \in (0, 1)$.

If the two miners adopt the strategy of cooperation at the same time, then the revenue per unit computational power per unit time of the entire mining pool increases to γR. The payoff of each miner is the difference between the reward which is proportional to its computational power and the cost to mine honestly. Therefore, under the strategy profile of (C, C), miner 1 has its payoff of $a_1\gamma R - C_1$ and miner 2 has its payoff of $a_2\gamma R - C_1$. If miner 1 mines honestly and miner 2 employs the BWH attack, that is the strategy profile is (C, A), then the actual useful computational power to dig up a legal block is a_1 and thus the total revenue per time of the mining pool is $a_1 R$. Under this situation, the pool manager first provides the additional reward to miner 1 to encourage its honest behavior, and then allocate the rest of reward $a_1(1-\delta)R$ to miner 1 and miner 2 proportional to their computational powers, respectively. So the payoff of miner 1 is $a_1\delta R + a_1^2(1-\delta)R - C_1$. Miner 2 could obtain a partial of reward as a free rider, even though it just consumes a smaller cost. Thus its payoff is $a_1 a_2(1-\delta)R - C_2$. For the strategy profile (A, C), the opposite symmetry case happens and then the payoffs of miner 1 and miner 2 are $a_1 a_2(1-\delta)R - C_2$ and $a_2\delta R + a_2^2(1-\delta)R - C_1$, respectively. For the last case of (A, A), as both of the miners attack, they cannot dig up a legal block, and thus no reward can be obtained. It follows that the payoff of each miner is $-C_2$.

Based on the above analysis and the aforementioned assumptions, the corresponding payoff matrix is shown in Table 1.

Table 1 Payoff matrix of the model

	Miner 2	
Miner1	Cooperate (C)	Attack (A)
Cooperate (C)	$a_1\gamma R - C_1,\ a_2\gamma R - C_1$	$a_1\delta R + (1-\delta)Ra_1^2 - C_1,\ (1-\delta)Ra_1a_2 - C_2$
Attack (A)	$(1-\delta)a_1a_2R - C_2,\ a_2\delta R + (1-\delta)a_2^2R - C_1$	$-C_2,\ -C_2$

2.2 The Solutions of the Evolutionary Game

In the established evolutionary game model, the two miners have two strategies and different payoffs. Let x and y, $0 \le x \le 1,\ 0 \le y \le 1$, be the probabilities of miner 1 and miner 2 to play the strategy of cooperation, respectively. Therefore, the possibilities to employ the BWH attack of miner 1 and miner 2 are $1-x$ and $1-y$, respectively.

Denote the payoffs of miner 1 when it takes the strategy of cooperation and adopts the BWH attack by U_{11} and U_{12}, respectively. According to the payoff matrix in Table 1, we can obtain U_{11} and U_{12} as follows:

$$\begin{aligned} U_{11} &= y(a_1\gamma R - C_1) + (1-y)[a_1\delta R + (1-\delta)Ra_1^2 - C_1]; \\ U_{12} &= y[(1-\delta)a_1a_2R - C_2] + (1-y)(-C_2). \end{aligned}$$

Hence, the average expected payoff of miner 1 is

$$\overline{U}_1 = xU_{11} + (1-x)U_{12}.$$

Similarly, let U_{21} and U_{22} be the payoffs of miner 2 when it mines honestly and employs the BWH attack, respectively. From the payoff matrix in Table 1, U_{21} and U_{22} are as follows:

$$\begin{aligned} U_{21} &= x(a_2\gamma R - C_1) + (1-x)[a_2\delta R + (1-\delta)Ra_2^2 - C_1]; \\ U_{22} &= x[(1-\delta)a_1a_2R - C_2] + (1-x)(-C_2). \end{aligned}$$

So, the average expected payoff of miner 2 is

$$\overline{U}_2 = yU_{21} + (1-y)U_{22}.$$

In an evolutionary game model, each participant keeps learning and then adjusts its lower-payoff strategy to the higher-payoff strategy. Such a learning approach results in a greatly significant growth rate of a strategy in a replicator system, which reflects the evolutionary direction. By [23], the growth rate of a strategy selected by a participant is just equal to the difference between the payoff of this strategy and its average expected payoff. Because $a_2 = \lambda a_1$, we have the replicator dynamic equations of miner 1 and miner 2 are as follows:

$$\begin{aligned} F(x,y) = \frac{\mathrm{d}x}{\mathrm{d}t} &= x(U_{11} - \overline{U}_1) = x(1-x)(U_{11} - U_{12}) \\ &= x(1-x)\big\{ \left[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R\right] y \\ &\qquad + a_1\delta R + (1-\delta){a_1}^2R - C_1 + C_2\big\}; \end{aligned} \tag{1}$$

$$\begin{aligned} G(x,y) = \frac{\mathrm{d}y}{\mathrm{d}t} &= y(U_{21} - \overline{U}_2) = y(1-y)(U_{21} - U_{22}) \\ &= y(1-y)\big\{\lambda\left[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R\right]x \\ &\quad + a_1\lambda\delta R + (1-\delta)\lambda^2{a_1}^2R - C_1 + C_2\big\}. \end{aligned} \tag{2}$$

Then, Equations (1) and (2) combine the following replicator dynamic system:

$$\begin{cases} F(x,y) = \dfrac{\mathrm{d}x}{\mathrm{d}t} = x(1-x)\{[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]y \\ \qquad\qquad + a_1\delta R + (1-\delta){a_1}^2R - C_1 + C_2\}; \\ G(x,y) = \dfrac{\mathrm{d}y}{\mathrm{d}t} = y(1-y)\{\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]x \\ \qquad\qquad + a_1\lambda\delta R + (1-\delta)\lambda^2{a_1}^2R - C_1 + C_2\}. \end{cases} \tag{3}$$

By the stability theorem of the differential equations, all the solutions satisfying $F(x,y) = \frac{\mathrm{d}x}{\mathrm{d}t} = 0$ and $G(x,y) = \frac{\mathrm{d}y}{\mathrm{d}t} = 0$ are the equilibrium points of the replicator dynamic system. It is not hard to see there are five fixed equilibrium points of this system: $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$ and (x^*,y^*), where

$$x^* = \frac{C_1 - a_1\lambda\delta R - (1-\delta)\lambda^2{a_1}^2R - C_2}{\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]}, \qquad y^* = \frac{C_1 - a_1\delta R - (1-\delta){a_1}^2R - C_2}{a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R},$$

if $x^* \in [0,1]$ and $y^* \in [0,1]$.

From the results in [23], we know the stability condition at the fixed equilibrium points can be achieved by the application of Jacobian matrix. Therefore, the Jacobian matrix of the replicator dynamic system (3) is:

$$\boldsymbol{J} = \begin{bmatrix} \frac{\partial F(x,y)}{\partial x} & \frac{\partial F(x,y)}{\partial y} \\ \frac{\partial G(x,y)}{\partial x} & \frac{\partial G(x,y)}{\partial y} \end{bmatrix},$$

where

$$\begin{aligned} &\frac{\partial F(x,y)}{\partial x} = (1-2x)\{[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]y + a_1\delta R + (1-\delta){a_1}^2R - C_1 + C_2\}; \\ &\frac{\partial F(x,y)}{\partial y} = x(1-x)[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]; \\ &\frac{\partial G(x,y)}{\partial x} = y(1-y)\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]; \\ &\frac{\partial G(x,y)}{\partial y} = (1-2y)\{\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]x + a_1\lambda\delta R + (1-\delta)\lambda^2{a_1}^2R - C_1 + C_2\}. \end{aligned}$$

The determinant (Det) and the trace (Tr) of $\boldsymbol{J}$ are as follows.

$$\begin{aligned} \mathrm{Det}\boldsymbol{J} = &(1-2x)(1-2y) \\ &\cdot \{[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]y + a_1\delta R + (1-\delta){a_1}^2R - C_1 + C_2\} \\ &\cdot \{\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]x + a_1\lambda\delta R + (1-\delta)\lambda^2{a_1}^2R - C_1 + C_2\} \\ &-xy(1-x)(1-y)\lambda[a_1(\gamma-\delta)R - (1-\delta)(1+\lambda){a_1}^2R]^2; \end{aligned}$$

$$\begin{aligned}\mathrm{Tr}\boldsymbol{J} = &(1-2x)\{[a_1(\gamma-\delta)R-(1-\delta)(1+\lambda){a_1}^2R]y+a_1\delta R+(1-\delta){a_1}^2R-C_1+C_2\}\\ &+(1-2y)\{\lambda[a_1(\gamma-\delta)R-(1-\delta)(1+\lambda){a_1}^2R]x+a_1\lambda\delta R+(1-\delta)\lambda^2{a_1}^2R-C_1+C_2\}.\end{aligned}$$

As different fixed equilibrium points bring different determinants and traces of the Jacobian matrix, we then list all determinants and traces in Table 2.

Table 2 The determinant and trace of the system at equilibrium points

	$\mathrm{Det}\boldsymbol{J}$	$\mathrm{Tr}\boldsymbol{J}$
$(0,0)$	$[\delta a_1R+(1-\delta)a_1^2R-C_1+C_2]$ $*[\delta\lambda a_1R+(1-\delta)\lambda^2a_1^2R-C_1+C_2]$	$[\delta a_1R+(1-\delta)a_1^2R-C_1+C_2]$ $+[\delta\lambda a_1R+(1-\delta)\lambda^2a_1^2R-C_1+C_2]$
$(0,1)$	$-[a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$ $*[\delta\lambda a_1R+(1-\delta)\lambda^2a_1^2R-C_1+C_2]$	$[a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$ $-[\delta\lambda a_1R+(1-\delta)\lambda^2a_1^2R-C_1+C_2]$
$(1,0)$	$-[\delta a_1R+(1-\delta)a_1^2R-C_1+C_2]$ $*[\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$	$-[\delta a_1R+(1-\delta)a_1^2R-C_1+C_2]$ $+[\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$
$(1,1)$	$[a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$ $*[\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$	$-[a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$ $-[\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2]$
(x^*,y^*)	θ	0

where

$$\begin{aligned}\theta = &-\left(1-\frac{C_1-a_1\lambda\delta R-(1-\delta)\lambda^2a_1^2R-C_2}{\lambda[a_1(\gamma-\delta)R-(1-\delta)(1+\lambda)a_1^2R]}\right)\left(1-\frac{C_1-a_1\delta R-(1-\delta)a_1^2R-C_2}{a_1(\gamma-\delta)R-(1-\delta)(1+\lambda)a_1^2R}\right)\\ &\cdot\left[C_1-a_1\lambda\delta R-(1-\delta)\lambda^2a_1^2R-C_2\right]\left[C_1-a_1\delta R-(1-\delta)a_1^2R-C_2\right].\end{aligned}$$

2.3 Equilibrium Analysis for the Evolutionary Game

Based on the results in [23], given a point (x,y), if the determinant $\mathrm{Det}\boldsymbol{J}(x,y)>0$ and the trace $\mathrm{Tr}\boldsymbol{J}(x,y)<0$, then this point is an evolutionary stable strategy. Thus according to Table 2.2, following five situations are necessary to be discussed.

Situation 1 When $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, then $\mathrm{Det}\boldsymbol{J}(1,1)>0$ and $\mathrm{Tr}\boldsymbol{J}(1,1)<0$, implying point $(1,1)$ is the unique evolutionary stable strategy. The main reason is as follows. From the condition of $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, it is easy to deduce that $a_1\gamma R-C_1>(1-\delta)Ra_1a_2-C_2$, since $a_2=\lambda a_1$ and $\lambda\in[0,1]$. It means that when miner 2 cooperates, then payoff of miner 1 when it cooperates is higher than the one when it attacks. On the other hand, from the condition of $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$, we know $a_1\delta R+(1-\delta)a_1^2R-C_1>-C_2$, implying that when miner 2 attacks, then payoff of miner 1 when it cooperates is also higher than the one when it attacks. Based on the analysis from two aspects, we can conclude that no matter whatever strategy miner 2 adopts, miner 1 always receives a higher benefit when it honestly mines. Therefore, miner 1 must be a cooperator. At this time, once miner 1 chooses cooperation, miner 2 adopts cooperation too, because $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$. Thus under this situation, the system is eventually evolved to adopt cooperation strategy by both miners and then $(1,1)$ is the evolutionary stable strategy.

Situation 2 When $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, we have $\mathrm{Det}\boldsymbol{J}(0,0)>0$, $\mathrm{Tr}\boldsymbol{J}(0,0)<0$ and $\mathrm{Det}\boldsymbol{J}(1,1)>0$, $\mathrm{Tr}\boldsymbol{J}(1,1)<0$. It means that $(0,0)$

and $(1,1)$ are both the evolutionary stable strategies of the system. Because of the condition of $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$, we can see that when miner 2 attacks, then playing the BWH attack is a better choice for miner 1, since it can obtain more payoff than the one when it cooperates. In addition, due to the condition that $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, it is not hard to observe that if miner 1 cooperates, then miner 2 selects the cooperation too. Thus the rational miners will choose to honestly mine if the cooperation can make them obtain higher payoffs. On the contrary, both of the participants choose to attack, if their payoffs are higher than the ones when they cooperate. So under this situation, the overall evolutionary results of the system are uncertain.

Situation 3 When $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, only solution $(0,0)$ satisfies $\mathrm{Det}\boldsymbol{J}(0,0)>0$ and $\mathrm{Tr}\boldsymbol{J}(0,0)<0$, meaning that $(0,0)$ is the unique stable point of the system. Based on the condition of $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$, we have $\lambda a_1\delta R+\lambda^2(1-\delta)a_1^2R-C_1<-C_2$ $(\lambda\in[0,1])$, showing that miner 2 can obtain higher payoff by attacking if miner 1 launches the BWH attack. From the condition of $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, it is easy to deduce that $\lambda a_1\gamma R-C_1<(1-\delta)\lambda a_1^2R-C_2$. It follows that miner 2 also can obtain higher payoff by attacking when miner 1 cooperates. Hence, miner 2 always attacks whatever the strategy miner 1 chooses. On the other hand, once miner 2 attacks, miner 1 selects to attack as $a_1\delta R+(1-\delta)a_1^2R-C_1<-C_2$. Therefore, under this situation, the system is eventually evolved to adopt attack strategy by both miners.

Situation 4 When $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, only the solution $(1,0)$ satisfies $\mathrm{Det}\boldsymbol{J}(1,0)>0$ and $\mathrm{Tr}\boldsymbol{J}z(1,0)<0$, meaning $(1,0)$ is the unique evolutionary stable strategy of the dynamic system. Since $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$, when miner 2 attacks, miner 1 can obtain more payoffs by cooperating. At the same time, when miner 1 mines honestly, the payoff of miner 2 to attack is higher than the one when it cooperates, due to $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$. Thus under this situation, the dynamic system is eventually evolved to $(1,0)$, that is adopting cooperation strategy by miner 1 and launching the BWH attack by miner 2.

Situation 5 When $a_1\lambda\delta R+(1-\delta)\lambda^2a_1^2R-C_1+C_2>0$ and $a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, then $(0,1)$ and $(1,0)$ are the stable points of the system. According to the conditions in this situation, we know that when miner 1 attacks, miner 2 gains more from honest mining, and when miner 1 honestly mines, miner 2 can gain a higher return by attacking. That is, when one side cooperates, the other side will choose to attack, and thus both sides will adopt different strategies. Under this situation, the dynamic system is eventually evolved to the state, in which one side adopts cooperation strategy and the other adopts attack strategy.

3 Computational Studies

3.1 Simulations for Different Situations

To help the readers to intuitively understand the conclusions of the evolutionary game model with the BWH attack, we first simulate the dynamic evolutionary process of two miners' strategy selection under different situations demonstrated in Subsection 2.3 by using Matlab.

1) Setting the parameters in the evolutionary game as: $\delta=0.2$, $a_1=0.6$, $a_2=\lambda a_1=0.4$, $\gamma=2$, $R=10$, $C_1=4$, $C_2=1$. Under this setting, it follows $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$ and

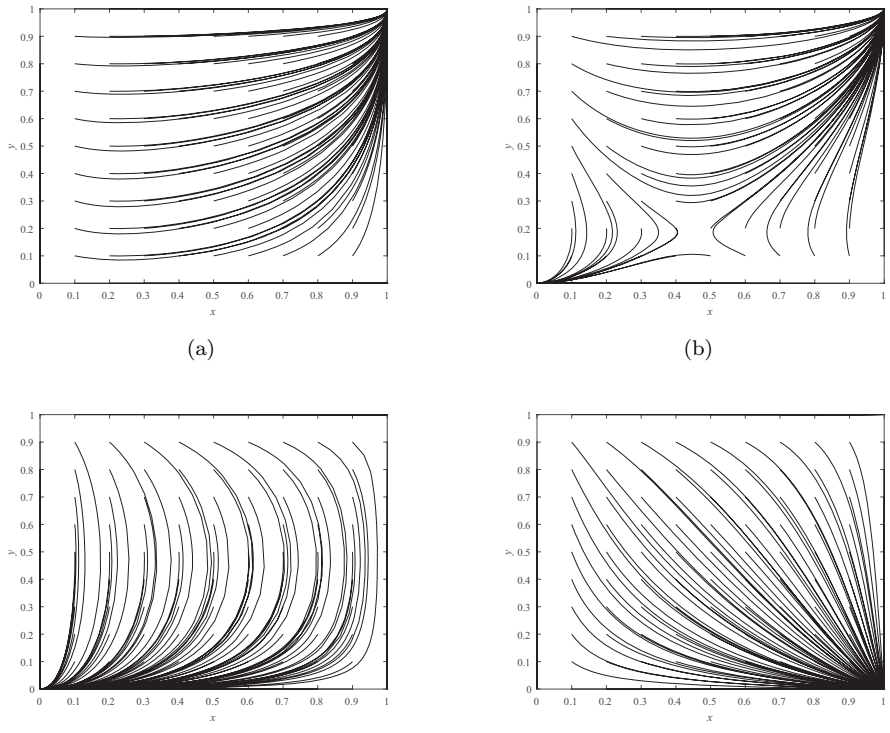
$\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, which is Situation 1. The dynamic evolutionary processes are shown in Figure 1(a), and the evolutionary stable strategy between the two miners is $(1,1)$.

2) Setting the parameters in the evolutionary game as: $\delta=0.2$, $a_1=0.5$, $a_2=\lambda a_1=0.4$, $\gamma=2$, $R=10$, $C_1=5$, $C_2=1$. Then $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$, $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2>0$, which is Situation 2. The dynamic evolutionary processes are shown in Figure 1(b). Obviously, $(0,0)$ and $(1,1)$ are the two evolutionary stable strategies of the system.

3) Setting the parameters in the evolutionary game as: $\delta=0.2$, $a_1=0.6$, $a_2=\lambda a_1=0.3$, $\gamma=2$, $R=10$, $C_1=7$, $C_2=0.5$. It follows $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2<0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, which is Situation 3. The dynamic evolutionary processes are shown in Figure 1(c), and then the system converges to the evolutionary stable strategy $(0,0)$.

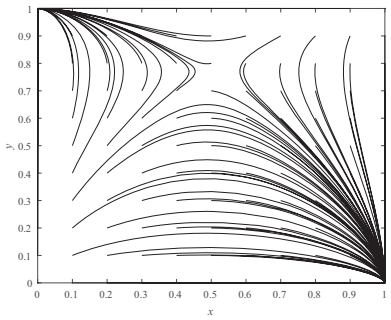
4) Setting the parameters in the evolutionary game as: $\delta=0.3$, $a_1=0.8$, $a_2=\lambda a_1=0.6$, $\gamma=1.2$, $R=10$, $C_1=7$, $C_2=1.5$. So $a_1\delta R+(1-\delta)a_1^2R-C_1+C_2>0$ and $\lambda a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$, which is Situation 4. Then the dynamic evolutionary processes between two parties are shown in Figure 1(d), and the evolutionary stable strategy is $(1,0)$.

5) Setting the parameters in the evolutionary game as: $\delta=0.2$, $a_1=1$, $a_2=\lambda a_1=0.9$, $\gamma=1.2$, $R=10$, $C_1=7$, $C_2=1$. Thus we have $a_1\lambda\delta R+(1-\delta)\lambda^2a_1^2R-C_1+C_2>0$ and $a_1\gamma R-(1-\delta)\lambda a_1^2R-C_1+C_2<0$. It just is Situation 4. Under this situation, the dynamic evolutionary processes between two parties are shown in Figure 1(e), and the the evolutionary stable strategies in the dynamic system are $(1,0)$ and $(0,1)$.



(a) (b)

(c) (d)



(e)

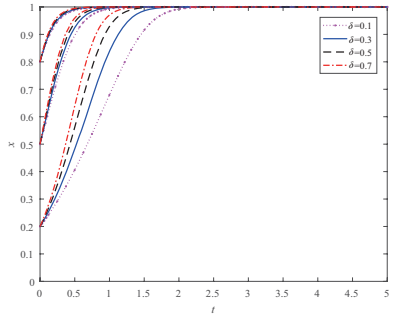
Figure 1 Dynamic evolution process of two miners

3.2 Simulations for the Influence of Parameters

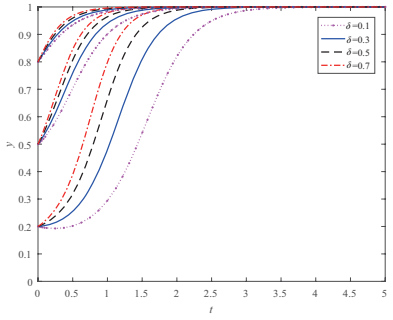
In the mining process, the main objective is to explore the cooperation tendency between two miners, that is the evolutionary stable strategy $(1, 1)$ is the ideal stable state which we expect for. In this subsection, we will discuss the influence of the parameters on both sides' strategic choice through analyzing the enlarging multiple γ of rewards, the percentage δ of additional rewards, and the ratio λ of the computational powers of two miners.

1) The influence of δ on the evolutionary behavior of miners.

In order to observe the impact of the additional rewards on the evolutionary behavior, we fix other parameters, and let δ take 0.1, 0.3, 0.5 and 0.7 respectively. Furthermore, the initial probability x, y takes 0.2, 0.5 and 0.8, respectively. Figure 2(a) and Figure 2(b) demonstrate that the additional reward mechanism can encourage miners to mine honestly. With the percentage δ of additional rewards increasing, the evolutionary speed of miner 1 and miner 2 toward cooperation strategy increases too. On the one hand, with a continuous increase of the additional rewards, the rate the miner evolves to the cooperation strategy gradually increases. On the other hand, after the additional rewards increased to a certain amount, the marginal effect would reduce. As a result, a certain additional reward mechanism can motivate miners to cooperation.



(a) Evolutionary behavior of miner 1



(b) Evolutionary behavior of miner 2

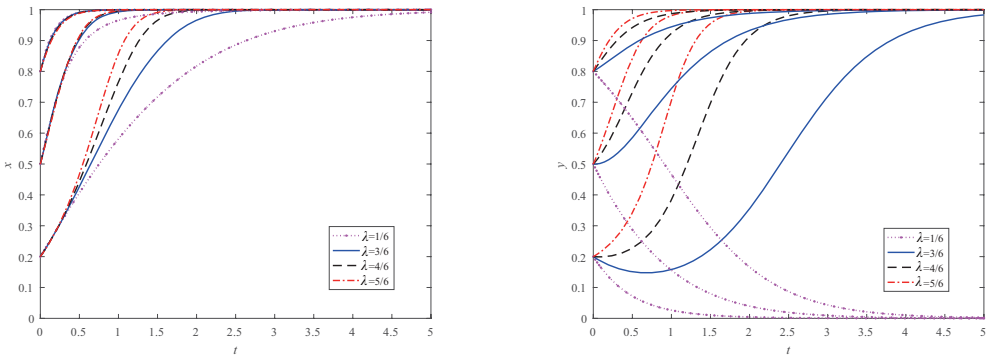
Figure 2 Impact of the percentage of additional rewards on the system evolution

2) The influence of λ on the evolutionary behavior of miners.

We fix the other parameters, and let λ take $\frac{1}{6}$, $\frac{3}{6}$, $\frac{4}{6}$ and $\frac{5}{6}$, respectively, to analyze the impact of the ratio λ of the computational power on the system evolution. The initial probability x and y take 0.2, 0.5 and 0.8, respectively. In Figure 3(a), we can observe that when the initial probability is low, the difference of the computational power between two miners has a great impact on the convergence speed of the miner 1's strategy. With the initial probability increasing, the difference of computational power has less influence on the convergence speed of miner 1's strategy. On the contrary, as shown in Figure 3(b), the changes of λ always have a significant impact on miner 2's strategy choice. When λ takes $\frac{1}{6}$, namely, the computational power of miner 2 is very small, it will adopts the BWH attack. With λ increasing, the miner 2 will turn from the BWH attack to honest mining. The higher the miners' computational power, the faster the miners' strategy converges to cooperation. Because of the higher computational power of miner 1, the rate it evolves to cooperation faster than that of miner 2. As a result, the higher computational power of the miner, the greater the probability to adopt a cooperation strategy.

3) The influence of γ on the evolutionary behavior of miners.

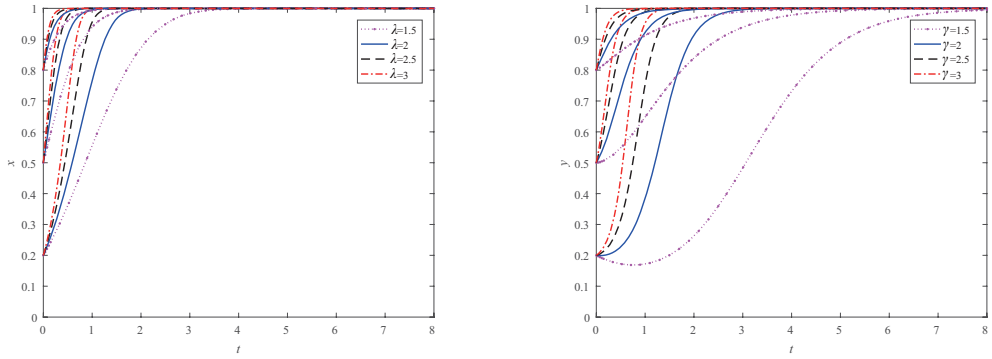
In order to observe the impact of the enlarging multiples of rewards on the evolutionary behavior, the other parameters are fixed, and γ takes 1.5, 2, 2.5 and 3 respectively. The initial probability x and y take 0.2, 0.5 and 0.8, respectively. With the gradual increase of the enlarging multiples of reward after the cooperation, the miners' strategy will converge to cooperate quickly. More precisely, from Figure 4, we can see that the enlarging multiples of rewards has a significant effect on miner 2. When γ takes 1.5, it takes a long time for miner 2 to evolve to be a cooperator. With γ increasing, miner 2 will turn to adopt a cooperation strategy regardless of the initial strategy selection. Comparing Figure 4(a) with Figure 4(b), the increased revenue caused by the cooperation strategy has an incentive effect on both parties, but the effect on lower computational power, such as miner 2, is more obvious.



(a) Evolutionary behavior of miner 1

(b) Evolutionary behavior of miner 2

Figure 3 Impact of the ratio of the computational power on the system evolution



(a) Evolutionary behavior of miner 1 (b) Evolutionary behavior of miner 2

Figure 4 Impact of the enlarging multiples on the system evolution

4 Conclusions

In this paper, we study the game evolution process of miners' behavior to adopt the BWH attack by leveraging evolutionary game theory. It focuses on the game evolution process and the influence of different parameters on the ideal stable states through numerical simulation.

In a mining pool, the manager prefers mitigating the BWH attack and promoting the miners to develop stable cooperative relationship, so as to improve the revenue of the pool, reduce the waste of the computational power and increase the efficiency of mining. For each miner, it shall make a choice to cooperate or attack, by comparing the amount of computational power it has with the other's. From the simulations in Section 3, we can make some recommendations for the manager and the miners. Firstly for the miner who equips with more computational power, it is much better for it to be a cooperator. Secondly, if the reward of the mining pool can be enlarged more under the strategy profile (C, C), then cooperation is a better choice for each miner. Thirdly, a proper additional reward mechanism can help the pool manager to encourage miners to mine honestly. While, there are some limitations in this paper, the model in this paper only focuses on the case containing two miners, and thus we will discuss the model containing more miners in the future.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. http://nakamotornstitute.org/bitcoin/, 2008.
[2] Lee S, Kim S. Countering block withholding attack efficiently. IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019: 330–335.
[3] Zhen Y, Yue M, Zhong-yu C, et al. Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus. 2017 36th Chinese Control Conference (CCC), 2017: 1441–1446.
[4] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014: 436–454.
[5] Kwon Y, Kim D, Son Y, et al. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017: 195–209.
[6] Eyal I. The miner's dilemma. 2015 IEEE Symposium on Security and Privacy, 2015: 89–103.
[7] Vasek M, Thornton M, Moore T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem.

International conference on financial cryptography and data security, Springer, Berlin, Heidelberg, 2014: 57–71.

[8] Rosenfeld M. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011.

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

[10] Luu L, Saha R, Parameshwaran I, et al. On power splitting games in distributed computation: The case of bitcoin pooled mining. 2015 IEEE 28th Computer Security Foundations Symposium, IEEE, 2015: 397–411.

[11] Schrijvers O, Bonneau J, Boneh D, et al. Incentive compatibility of bitcoin mining pool reward functions. International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2016: 477–498.

[12] Bag S, Sakurai K. Yet another note on block withholding attack on bitcoin mining pools. International Conference on Information Security, Springer, Cham, 2016: 167–180.

[13] Bag S, Ruj S, Sakurai K. Bitcoin block withholding attack: Analysis and mitigation. IEEE Transactions on Information Forensics and Security, 2016, 12(8): 1967–1978.

[14] Wu D, Liu X, Yan X, et al. Equilibrium analysis of bitcoin block withholding attack: A generalized model. Reliability Engineering & System Safety, 2019, 185: 318–328.

[15] Cardell J B, Hitt C C, Hogan W W. Market power and strategic interaction in electricity networks. Resource and Energy Economics, 1997, 19(1–2): 109–137.

[16] Taylor P D, Jonker L B. Evolutionary stable strategies and game dynamics. Mathematical Biosciences, 1978, 40(1–2): 145–156.

[17] Smith J M. The theory of games and the evolution of animal conflicts. Journal of Theoretical Biology, 1974, 47(1): 209–221.

[18] Liu X, Wang W, Niyato D, et al. Evolutionary game for mining pool selection in blockchain networks. IEEE Wireless Communications Letters, 2018, 7(5): 760–763.

[19] Wang Y, Tang C, Lin F, et al. Pool strategies selection in PoW-based blockchain networks: Game-theoretic analysis. IEEE Access, 2019, 7: 8427–8436.

[20] Kim S, Hahn S G. Mining pool manipulation in blockchain network over evolutionary block withholding attack. IEEE Access, 2019, 7: 144230–144244.

[21] Cheng Y K, Xu Z Q. Study on the block withholding attack based on the evolutionary game. Journal of Xidian University, 2020, 47(5): 1–11.

[22] Tang C B, Yang Z, Zheng Z L, et al. Game dilemma analysis and optimization of PoW consensus algorithm. Acta Automatica Sinica, 2017, 43(9): 1520–1531.

[23] Friedman D. On economic applications of evolutionary game theory. Journal of Evolutionary Economics, 1998, 8(1): 15–43.