International Journal of Computational Intelligence Systems
Vol. **12(2)**, 2019, *pp.* 1353–1360
DOI: https://doi.org/10.2991/ijcis.d.191030.001; ISSN: 1875-6891; eISSN: 1875-6883
https://www.atlantis-press.com/journals/ijcis/

A Biform Game Approach to Preventing Block Withholding Attack of Blockchain Based on Semi-CIS Value

Xiao-Li Du[1], Deng-Feng Li[2,*], Kai-RongLiang[1,*]

[1]*School of Economics and Management, Fuzhou University, No. 2, Xueyuan Road, Daxue Town, Fuzhou, Fujian, 350108, China*
[2]*School of Management and Economics, University of Electronic Science and Technology of China, No. 2006, Xiyuan Road, High-Tech District, Chengdu Sichuan, 611731, China*

ARTICLE INFO

Article History
Received 28 Sep 2019
Accepted 28 Oct 2019

Keywords
Blockchain
Mining pool
Block withholding attack
Biform game
Big data

ABSTRACT

In proof-of-work (PoW)-based blockchain network, the blockchain miners publish blocks by contributing computing power to solve crypto-puzzles. Due to the weak computing power of single miner, miners tend to join a mining pool and share the profits from the mining pool according to the contribution proportions of the miners. However, some miners may initiate block withholding attack which may result in wasting computing power, even threatening the efficiency of the blockchain network. To address this problem, in this paper, we use the biform game model to optimize the miners' strategy choices. We firstly formulate the mining process as a non-cooperative–cooperative biform game model. We use the model to exhibit miners' strategy choices (non-cooperation stage) and the cooperation mining process (cooperation stage). Then we set the conditions to maintain the voluntary honest behavior of miners. After that, we employ the semi-CIS (semi-the center of imputation set value) value to compute the solutions of the cooperative games in the cooperation stage, and optimize miners' strategy choices to prevent the block withholding attack. Hence we can ensure the blockchain network is secure. Finally, the validity and applicability of the proposed model and method are verified by a numerical example.

1. INTRODUCTION

In recent years, blockchain technology has received extensive attention due to its auditability, immutability, security and anonymity. But strictly speaking, the technology is immature. There are many security problem. As the typical application, bitcoin has been running steadily for many years. However, the blockchain mining security issue is remain tough. With the increasing popularity of the blockchain technology, the blockchain mining has attracted more and more attention. And the proof-of-work (PoW) is a commonly used consensus mechanism for blockchain mining. Its operation principle is as follows: miners publish blocks by contributing computing power to solve crypto-puzzles and acquire profits when solving successfully. Since the blockchain system generates one block about 10 minutes, it is difficult for most miners to produce a block in a given period of time. In order to increase the possibility of obtaining stable profits, miners will choose to join the open mining pool for computational share (i.e., cooperative mining). Specifically, the miners acquire profits through accepting the less difficult tasks released by the mining pool manager and submitting the PoWs to the mining pool manager. However, in the mining pool system, there are some miners may initiate block withholding attack. This attack is an action that the attackers only submit partial PoWs (PPoWs) to the mining pool manager as the computational share. They will not submit the integral PoWs, but discard them when they find the integral PoWs. When the mining pool manager detects that the mining pool is suffering from block withholding attack, it is very difficult to identify the attacking miners. So without contributing the integral computing power, the attackers obtain profits from the mining pool, which result in reducing the profit of the mining pool and wasting computing power, even threatening the efficiency of the blockchain network. To address this challenge, Sarker *et al.* [1] and Tosh *et al.* [2] researched the solutions to this problem from the perspective of mining rewards model improvement. Siamak and Maria [3] and Chang and Park [4] improved the timestamp technology to prevent the block withholding attack. Meanwhile, to prevent block withholding attack, a solution to model the mining process as a stochastic game has been investigated [5], which used the reinforcement learning method to simulate the mining pools how to launch the block withholding attacks. Wang *et al.* [6] researched the mining process with a two-stage game model and analyzed the existence conditions of the Nash equilibrium and strategy choice stability. Tang *et al.* [7] applied non-cooperative iterated game to analyze miners behaviors, and resorted Zero-Determinant (ZD) strategy to design strategy mechanism to solve the tragedy of the commons problem in mining pool. Similarly, Hu *et al.* [8] applied the ZD strategy to analyze the strategy choices of arbitrary two mining pools to stop block withholding attack, and the application conditions of ZD strategy was given and the validity of the method was

* *Corresponding authors. Email: liangkr2017@163.com, lidengfeng@uestc.edu.cn*

verified. Wu *et al.* [9] employed pure strategy and hybrid strategy to prove that information hiding mechanism which can increase information asymmetry can reduce the occurrence of block withholding attack. Bag *et al.* [10] proposed cryptographic commitment schemes combined the hash function to counter block withholding attack. According to the above analysis, we can learn that the non-cooperative game or the evolutionary game method is generally used to avoid the block withholding attack in the mining pool.

In actual mining process, miners are not just the single relationship of competition or cooperation. The relationship among them is showing the interweaving of competition and cooperation. That means cooperation in competition and competition in cooperation. So a single non-cooperative or cooperative game approach is not well used to demonstrate the essence of the mining problem. In view of this, we adopt the concept of the biform game that was firstly proposed in 2007 by Brandenburger and Stuart [11] to research the strategy optimization of miners to avoid block withholding attack. This kind of game is mainly divided into two stages: the first stage is the non-cooperative game, the players in the game choose strategies and form the strategy situations, but the strategy situations only form the competitive environment of the second stage, not directly generate payments; the second stage is the cooperative game, the players cooperate and form coalitions in the strategy situations which formed in the first stage. Moreover, this stage distributes benefits among the players, and the benefit allocation values are as the payments of the players in the first stage.

Generally, the non-cooperative game and cooperative game are used to solve different problems. The non-cooperative game is to solve the strategy choice problems. Specifically, it is to study how the players make decisions to maximize their own benefits in the interactional situation. And it does not consider whether the players cooperate with each other and how to distribute cooperative incomes. While the cooperative game is to solve income distribution problems. It studies how to distribute the benefits among people when they reach cooperation. And the cooperative game does not consider the strategy choice problems. In reality, the miners want to obtain the benefits brought by the strategy when they make strategy choices. The biform game realizes the combination of the non-cooperative game and cooperative game. So it can be used to solve the game problems including both strategy selection and profit distribution. That is to say, the miners can obtain the strategy and the benefits brought by the strategy at the same time, rather than just acquiring one of the two.

Since the introduction of the biform game theory, its theoretical and applied research has been in the ascendant. Such as, Ryall and Sorenson [12] analyzed the competition problem of agents in the framework of biform game. Gui *et al.* [13] used the biform game approach to construct an incentive mechanism to encourage producers to participate in the design of recyclable products. Mahjoub and Hennet [14] applied the biform game to describe the supply network design problem under the market expectation price elasticity demand. Feess and Thun [15] researched the biform game model based on the Shapley value, and used it to solve the strategy choice and revenue distribution problems in the supply chain. Kim [16] solved the low flexibility and adaptability problem of wireless body area network (WBAN) by building a WBAN resource sharing reverse-biform game model. In this paper, we formulate the mining process as a biform game model to optimize miners' strategy choices. For the two stages of the non-cooperative–cooperative biform game, we employ the semi-CIS (semi-the center of imputation set value) value to compute the solutions of the cooperative games in the cooperation stage. And the obtained benefit allocation values are as the payments of the players in the non-cooperation stage. Then the pure strategy Nash equilibrium solution in the non-cooperation stage is obtained. Special emphasis on one point: the biform game method can always guarantee to be the pure strategy Nash equilibrium solution, while the Nash equilibrium of the non-cooperative game is a mixed strategy in most cases. Due to the fact that the mixed strategy cannot be implemented or applied well in practical problems, we apply the biform game model to better instruct miners to choice strategy. Finally, we achieve the goal of preventing block withholding attack.

The rest of this paper is organized as follows. Section 2 constructs the mining pool biform game model. This section describes the problem of miners strategy choices in the non-cooperation stage, the problem of miners mining in cooperation stage and the characteristic functions of cooperative games. On the basis of the definitions and properties of the semi-CIS value in the cooperation stage and the Nash equilibrium solutions in the non-cooperation stage, the solving method and procedures of the mining pool biform game model are summarized in Section 3. In Section 4, the validity and applicability of the proposed model and method are verified by a numerical example. Finally, the conclusions are stated in Section 5.

2. SYSTEM MODELS

2.1. Miner Strategy Choice in Non-Cooperation Stage

There are n miners in a mining pool, where the miners are regarded as the players. Let $N = \{1, 2, 3, ..., n\}$ be the finite miner (i.e., player) set, where i ($i \in N$) is the ith miner and $n \geq 3$. For the block withholding attack, the strategy choices of miners can be expressed as two types: the malicious strategy which means the miners discard the integral PoWs when they find them and share the profit from the mining pool with submitting the partial PoWs, and the honest strategy which means the miners honestly mine and submit completed PoWs to the mining pool manager. When a small part of miners choose the malicious strategy but other miners do not choose this strategy, they can continuously acquire mining profits. That is, miners can initiate block withholding attack to increase their own profits. But the profits of the miners with the honest strategy are reduced due to the attack action. Besides, it is worth noting the available computing power of the mining pool decides the probability of the mining pool to gain a profit. If all the miners choose the malicious strategy, they will get nothing. Therefore, miners will make strategy choices to maximize their own profits during the mining process. Let $G_i = \{0, 1\}$ denote the miner i's strategy set, and $S_k = (g_{k1}, g_{k2}, \dots, g_{ki}, \dots, g_{kn}) \in \{0, 1\}^n$ denote the kth situation, where the miner $i \in N$, and $g_{ki} \in G_i = \{0, 1\}$. $g_{ki} = 0$ means the miner i chooses the malicious strategy in the situation k; while $g_{ki} = 1$ means the miner i chooses the honest strategy in the situation k.

All of the miners will form 2^n situations when n miners respectively choose their own strategies. Such as, there are three miners 1, 2, and 3 in the mining pool, and there will form $2^3 = 8$ situations. The details are shown in Table 1.

The situation $S_1 = (0,0,0)$ denotes all the miners choose the malicious strategy. And the situation $S_2 = (0,1,0)$ means the miner 2 chooses the honest strategy while both the miner 1 and miner 3 choose the malicious strategy. Thus, the meaning of other situations can be interpreted by the similar way.

2.2. Problem and Method in Cooperation Stage

The first stage is non-cooperation in biform game model which is different from the two-stage game model due to payoffs unknown a prior. We have cooperation rather than non-cooperation second-stage games for the following reasons.

In the mining pool system, the mining pool manager divides the mining task into a number of subtasks which are less difficult and sends them to the miners. Then the miners receive the subtasks and submit the completed PoWs to the mining pool manager, which means that the miners participate in cooperative mining. So how to pay profits to the cooperative miners is a cooperative game problem, where the miners are regarded as the players. Another reason is that the benefits of miners participating in mining cooperation are more than those they do alone.

In addition, the payoff values of the two-stage game can be directly determined in the first non-cooperation stage, while those of the biform game are computed based on the calculation results of second cooperation stage.

In this paper, the cooperative game is expressed as $(N, V(S_k))$, where $V(S_k)$ denotes the profit function (or characteristic function) in the situation S_k. Stated as above, miners may choose honest or malicious strategy. Thereby, considering the influence of the miners with the honest strategy, the profit function is constructed as the following rule. That is, the greater the number of the miners with the honest strategy in the mining pool, the higher the probability for the mining pool to mine successfully, and the higher probability for the mining pool to win a mining competition with other mining pools in the blockchain network. To prevent miners from choosing the malicious strategy, we restrict miners behaviors by adjusting the cost per unit computing power. The details are given as follows: for any coalition $T \subseteq N$, the profit function $V(S_k)(T)$ of T in the situation S_k can be expressed as

$$V(S_k)(T) = (R+\theta s)\frac{1}{w}\left(\sum_{i_h \in H \subseteq T} w_{i_h} + \sum_{j_m \in T\backslash H} \gamma w_{j_m}\right)\frac{1}{w_G} \quad (1)$$

$$\sum_{i_h, j_m \in T}\left(w_{i_h} + w_{j_m}\right) - \left(\sum_{i_h \in H \subseteq T} \lambda w_{i_h} + \sum_{j_m \in T\backslash H} \lambda\gamma w_{j_m}\right)$$

The definitions of the parameters used in Eq. (1) are listed in Table 2.

Further, $\omega_{i_h} = \omega_i$ and $\omega_{j_m} = \omega_j$, where ω_i is the computing power of the miner i determined by the built-in chip of its mining machine and ω_j is the computing power of the miner j. By using the sub-subscripts m and h to denote the miner's strategy choice. Then the costs of cooperative mining for the miner i with the honest strategy and the miner j with the malicious strategy are denoted by $\lambda\omega_{i_h}$ and $\gamma\lambda\omega_{j_m}$, respectively. $\omega_G = \sum_{i,j \in N}\left(\omega_i + \omega_j\right)$ denotes the sum of the computing power of all the miners in the mining pool. That is, it is the computing power of the mining pool, which can be obtained by the mining pool detection technology. In this study, we consider is the situation of a single mining pool. So we can take it as constant when the mining pool is determined and the number of miners in

Table 1 The strategy situations of three miners with two strategies.

Strategies		Miner 3			
		0		1	
		Miner 2		Miner 2	
		0	1	0	1
Miner 1	0	$S_1 = (0,0,0)$	$S_2 = (0,1,0)$	$S_3 = (0,0,1)$	$S_4 = (0,1,1)$
	1	$S_5 = (1,0,0)$	$S_6 = (1,1,0)$	$S_7 = (1,0,1)$	$S_8 = (1,1,1)$

Table 2 Parameters and their definitions.

Parameter	Definition
R	The fixed token-issuing reward decided by the blockchain network
θ	The transaction confirmation price per unit data size decided by the blockchain users
s	The block size decided by the number of transactions
$H \subseteq T$	The set of the miners with the honest strategy in the coalition T
$T\backslash H$	The set of the miners with the malicious strategy in the coalition T
$i_h\ (i_h \in H \subseteq T)$	The miner $i\,(i \in N)$ chooses the honest strategy in the coalition T
$j_m (j_m \in T\backslash H)$	The miner $j\,(j \in N)$ chooses the malicious strategy in the coalition T
ω	The total computing power of the blockchain network, which can be obtained by multiplying The number of miners by the average computing power of the miners
ω_{i_h}	The computing power of the miner i with the honest strategy
ω_{j_m}	The computing power of the miner j with the malicious strategy
ω_G	The computing power of the mining pool
$\gamma\ (0 \le \gamma < 1)$	The proportion of the submitted PoWs when the miners choose the malicious strategy
λ	The cost per unit computing power decided by the mining pool system

the mining pool is fixed. $\sum_{i_h \in H \subseteq T} \omega_{i_h}$ is the total computing power of the miners with the honest strategy in the coalition T. $\sum_{j_m \in T \backslash H} \gamma\omega_{j_m}$ is the total computing power of the miners with the malicious strategy in the coalition T. $\left(\sum_{i_h \in H \subseteq T} \omega_{i_h}\right)/\omega$ is the probability of the coalition T to win a mining competition in the blockchain network. $\left[\sum_{i_h, j_m \in T} \left(\omega_{i_h} + \omega_{j_m}\right)\right]/\omega_G$ is the profit probability of the coalition T in the mining pool, which decides the profit allocation of the coalition T.

Theorem 1. *Assume that $(R+\theta s)/\omega$ is constant. Then, for any coalition $T \subseteq N$, the more miners with the honest strategy in the coalition, the more profit of the coalition obtain if $0 < \lambda < [(R+\theta s)\omega_l]/(\omega\omega_G)$, where $\omega_l = min\{\omega_i\}$.*

Proof. Give a miner p $\left(p \in H \subseteq T\right)$ with the honest strategy in the coalition T, then the profit of the coalition T is

$$V(S_k)(T) = (R+\theta s)\frac{1}{\omega}\left(\sum_{i_h \in H \subseteq T} \omega_{i_h} + \sum_{j_m \in T \backslash H} \gamma\omega_{j_m}\right)$$

$$\frac{1}{\omega_G}\sum_{i_h, j_m \in T}\left(\omega_{i_h} + \omega_{j_m}\right) - \left(\sum_{i_h \in H \subseteq T} \lambda\omega_{i_h} + \sum_{j_m \in T \backslash H} \gamma\lambda\omega_{j_m}\right).$$

If the miner p changes the strategy to the malicious strategy, then the profit of the coalition T is

$$V'(S_k)(T) = (R+\theta s)\frac{1}{\omega}\left(\sum_{i'_h \in H' \subseteq T} \omega_{i'_h} + \sum_{j'_m \in T \backslash H'} \gamma\omega_{j'_m}\right)$$

$$\frac{1}{\omega_G}\sum_{i'_h, j'_m \in T}\left(\omega_{i'_h} + \omega_{j'_m}\right) - \left(\sum_{i'_h \in H' \subseteq T} \lambda\omega_{i'_h} + \sum_{j'_m \in T \backslash H'} \gamma\lambda\omega_{j'_m}\right),$$

where, $H' = H \backslash p$. The strategy choice of the miner p is changed, but the number of miners in the coalition T is unchanged, so we have

$$\sum_{i'_h, j'_m \in T}\left(\omega_{i'_h} + \omega_{j'_m}\right) = \sum_{i_h, j_m \in T}\left(\omega_{i_h} + \omega_{j_m}\right).$$

Therefore, we have

$$\begin{aligned}
V(S_k)(T) - V'(S_k)(T) &= (R+\theta s)\frac{1}{\omega}\left(\sum_{i_h \in H \subseteq T} \omega_{i_h} + \sum_{j_m \in T \backslash H} \gamma\omega_{j_m} - \sum_{i'_h \in H' \subseteq T} \omega_{i'_h} - \sum_{j'_m \in T \backslash H'} \gamma\omega_{j'_m}\right) \\
&\quad \frac{1}{\omega_G}\sum_{i_h, j_m \in T}\left(\omega_{i_h} + \omega_{j_m}\right) - \sum_{i_h \in H \subseteq T} \lambda\omega_{i_h} + \sum_{i'_h \in H' \subseteq T} \lambda\omega_{i'_h} \\
&\quad + \sum_{j'_m \in T \backslash H'} \gamma\lambda\omega_{j'_m} - \sum_{j_m \in T \backslash H} \gamma\lambda\omega_{j_m} \\
&= (R+\theta s)\frac{1}{\omega}\left(\sum_{i'_h \in H' \subseteq T} \omega_{i'_h} + \omega_{p_h} - \sum_{i'_h \in H' \subseteq T} \omega_{i'_h} \right. \\
&\quad \left. + \sum_{j_m \in T \backslash H} \gamma\omega_{j_m} - \sum_{j_m \in T \backslash H} \gamma\omega_{j_m} - \gamma\omega_{p_m}\right)\frac{1}{\omega_G} \\
&\quad \sum_{i_h, j_m \in T}\left(\omega_{i_h} + \omega_{j_m}\right) - \sum_{i'_h \in H' \subseteq T} \lambda\omega_{i'_h} - \lambda\omega_{p_h} \\
&\quad - \sum_{j_m \in T \backslash H} \gamma\lambda\omega_{j_m} + \sum_{i'_h \in H' \subseteq T} \lambda\omega_{i'_h} + \sum_{j_m \in T \backslash H} \gamma\lambda\omega_{j_m} + \gamma\lambda\omega_{p_m} \\
&= (R+\theta s)\frac{\omega_p}{\omega\omega_G}(1-\lambda)\sum_{i_h, j_m \in T}\left(\omega_{i_h} + \omega_{j_m}\right) - \lambda\omega_p(1-\gamma).
\end{aligned}$$

If $0 < \lambda < [(R+\theta s)\omega_l]/(\omega\omega_G)$, where $\omega_l = min\{\omega_i\}$, we can obtain $V_m(S_k)(T) - V'_m(S_k)(T) > 0$, which means the more miners with the honest strategy in the coalition, the more profit of the coalition obtained.

For example, a coalition $U(U \subseteq N)$ which has b $\left(b \le |U|\right)$ miners with the honest strategy can obtain the profit $V(S_k)(U)$. If the number of the miners with the honest strategy is decreased to $b-1$, the profit of the coalition U is $V'(S_k)(U)$, then we have $V(S_k)(U) > V'(S_k)(U)$.

If $T = \{i\}$, there is only one miner in the coalition, then the profit of the coalition is

$$V(S_k)(i) = V(S_k)(\{i\}) = \frac{1}{\omega}(R+\theta s)\frac{\omega_i^2}{\omega_G} - \lambda\omega_i,$$

when the miner i chooses the honest strategy.

Simultaneously, the profit of the coalition is

$$V(S_k)(i) = \frac{1}{\omega}(R+\theta s)\frac{\gamma\omega_i^2}{\omega_G} - \lambda\gamma\omega_i,$$

when the miner i chooses the malicious strategy.

If $T = N$, i.e., the grand coalition consists of all the miners, then the profit of the grand coalition is

$$V(S_k)(N) = \frac{\omega_G}{\omega}(R+\theta s) - \lambda\omega_G,$$

when all the miners choose the honest strategy.

Simultaneously, the profit of the grand coalition is

$$V(S_k)(N) = \frac{\gamma\omega_G}{\omega}(R+\theta s) - \lambda\gamma\omega_G,$$

when all the miners choose the malicious strategy.

3. MODEL SOLVING METHOD AND PROCEDURES

In this section, based on the analysis of the definitions and properties of the semi-CIS value in the cooperation stage and the Nash equilibrium solutions in the non-cooperation stage, the solving method and procedures of the mining pool biform game model are proposed.

3.1. Semi-CIS Value

The semi-CIS value is one of important single-valued solutions of cooperative games. It first assigns each player (i.e., miner) to individual worth, and then distributes the remaining income of the grand coalition equally among all players [17,18].

Definition 1. For a n-person (i.e., miner) cooperative game $(N, V(S_k))$, where S_k is the situation, $N = \{1, 2, ..., n\}$ is the finite player (i.e., miner) set and $V(S_k)$ is the characteristic function, the semi-CIS value is a n-dimensional vector, i.e., $\boldsymbol{SCIS}(V(S_k)) = (SCIS_1(V(S_k)), SCIS_2(V(S_k)), ..., SCIS_n(V(S_k)))^{\mathrm{T}}$.

Here, for any player $i \in N$, there is

$$SCIS_i(V(S_k)) = \alpha_i[V(S_k)(\{i\})] + \frac{1}{n}\left\{V(S_k)(N) - \sum_{j\in N, j\neq i}\alpha_j[V(S_k)(\{j\})]\right\} \quad (2)$$

where $\alpha_j \in [0, 1]$ is the selfish level which indicate the participation cooperative possibility of any player $j \in N$ in the game. Eq. (2) is the semi-CIS value of any player i in the cooperative game $(N, V(S_k))$.

The calculation of the semi-CIS value is only related to the values of the grand coalition and the individuals, not related to other intermediate coalitions' values. This is similar to the real miner's profit calculation, which the miner's profit concerns only about the computing power of each miner contributing and the entire computing power of the mining pool.

The semi-CIS value satisfies collective effectiveness. Namely,

$$\sum_{i\in N} SCIS_i(V(S_k)) = V(S_k)(N).$$

Definition 2. For any players $i, j \in N$ and $i \in M, j \notin M, M \subseteq N$, the maximal complaint of the player $i \in M$ over another player $j \notin M$ at the payoff vector $\boldsymbol{SCIS}(M, V(S_k))$ is defined by the maximal complaint among coalitions containing the player i, but not the player j. That is,

$$m_{ij}^{v}(\alpha, \boldsymbol{SCIS}) = max\left\{\hat{e}(M, \boldsymbol{SCIS}) = \sum_{i\in M} SCIS_i(V(S_k)(M)) - \sum_{i\in M}\alpha_i[V(S_k)(\{i\})] \,|M \subseteq N, i \in M, j \notin M\right\},$$

where $SCIS_i(V(S_k)(M))$ is the real profit allocation value of the player i in the coalition M, and $\alpha_i[V(S_k)(\{i\})]$ is the proportion allocation value of the player i in the coalition M when it does alone. Moreover, for any players $i, j \in N$, if $m_{ij}^{v}(\alpha, \boldsymbol{SCIS}) = m_{ji}^{v}(\alpha, \boldsymbol{SCIS})$, then the semi-CIS value satisfies equal maximal complaint property.

Definition 3. Assume that there exist two cooperative games $(N, V(S_k))$ and $(N, W(S_k))$ such that they satisfy $\alpha_i[V(S_k)(\{i\})] \geq \alpha'_i[V(S_k)(\{i\})]$, where $i \in N$. If $SCIS_i(V(S_k)) \geq SCIS_i(W(S_k))$, then the semi-CIS value satisfies semi individual monotonicity property.

Definition 4. Assume that there exist a α–inessential games $(N, V(S_k)) = \sum_{i\in N}\alpha_i[V(S_k)(\{i\})], |N| \geq 2$, where $i \in N$. If $SCIS_i(V(S_k)) = \alpha_i[V(S_k)(\{i\})]$, then the semi-CIS value satisfies semi inessential game property.

According to Definitions 1–4, it is straightforward to prove the following conclusion, i.e., Theorem 2 (Here we omit the proof).

Theorem 2. *The semi-CIS value is the unique value, which satisfies efficiency, equal maximal complaint property, linearity, semi inessential game property, and semi individual monotonicity.*

3.2. Nash Equilibrium Solutions in Non-Cooperation Stage

Definition 5. For a biform game $(S_1, S_2, ..., S_m; V)$, where m is the total number of situations that can be formed and $N = \{1, 2, ..., n\}$ is the finite player set, G_i is the strategy set of any player $i \in N$ and $V(S_k)$ is the characteristic function, we assume there exists a situation $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{ik^*}, ..., s_{nk^*}), (k^* \in \{1, 2, ..., m\})$, where s_{ik^*} is the strategy of the player $i \in N$ in the situation k^* and $s_{ik^*} \in G_i$, for each player i in any situation $(r_i, \boldsymbol{s}_{-ik^*}) = (s_{1k^*}, s_{2k^*}, ..., s_{i-1,k^*}, r_i, s_{i+1,k^*}, ..., s_{nk^*})$, where $r_i \in G_i$ and $\boldsymbol{s}_{-ik^*} = (s_{1k^*}, s_{2k^*}, ..., s_{i-1,k^*}, s_{i+1,k^*}, ..., s_{nk^*})$ in $\boldsymbol{G}_{-i}$, if the following inequality is valid

$$SCIS_i(V(S_{k^*})) = \alpha_i[V(S_{k^*})(\{i\})] + \frac{1}{n}[V(S_{k^*})(N) - \sum_{j\in N, j\neq i}\alpha_j[V(S_{k^*})(\{j\})] \geq SCIS_i(V(r_i, \boldsymbol{s}_{-ik^*}))$$

then $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*})$ is called the pure strategy Nash equilibrium of the biform game $(S_1, S_2, ..., S_m; V)$. And the corresponding Nash equilibrium value $SCIS_i(V(S_{k^*}))$ is the profit of the player $i \in N$ in the situation S_{k^*}. Hereby, the Nash equilibrium solution of the biform game $(S_1, S_2, ..., S_m; V)$ is $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$.

Definition 6. $S_{k^*} \in \{S_1, S_2, ..., S_m\}$ is the effective strategy situation of the biform game $(S_1, S_2, ..., S_m; V)$ if $V(S_{k^*})(N) = \max_{1\leq k\leq m}\{V(S_k)(N)\}$.

Obviously, Definition 6 means the profit of the grand coalition reaches the maximum value in the effective strategy situation.

Further, we can prove the following three conclusions by using Definitions 1–6.

Theorem 3. *Assume that the characteristic function of the biform game $(S_1, S_2, ..., S_m; V)$ satisfies efficiency and equal maximal complaint property. For any strategy $r_i \in G_i (i = 1, 2, ..., n)$, if $V(S_{k^*})(N) \geq V(r_i, \boldsymbol{s}_{-ik^*})(N)$, where $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*}), (k^* \in \{1, 2, ..., m\})$, then $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ is the Nash equilibrium solution of the biform game $(S_1, S_2, ..., S_m; V)$.*

Corollary 1. For any strategy $r_i \in G_i (i = 1, 2, ..., n)$, if $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ is the Nash equilibrium solution of the biform game $(S_1, S_2, ..., S_m; V)$, then we can obtain $V(S_{k^*})(N) \geq V(r_i, \boldsymbol{s}_{-ik^*})(N)$.

Theorem 4. *Assume that the characteristic function of the biform game* $(S_1, S_2, ..., S_m; V)$ *satisfies Independence property (ID) and No coordination property (NC). If* $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ *is the Nash equilibrium solution of the biform game* $(S_1, S_2, ..., S_m; V)$*, then* $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*})$ *is an effective strategy situation.*

Theorem 5. *Assume that the characteristic function of the biform game* $(S_1, S_2, ..., S_m; V)$ *satisfies ID. If* $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*})$ *is an effective strategy situation, then* $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ *is the Nash equilibrium solution of the biform game* $(S_1, S_2, ..., S_m; V)$.

Corollary 2. Assume that the characteristic function of the biform game $(S_1, S_2, ..., S_m; V)$ satisfies $V(S_k)(\{j\}) = V(r_i, \boldsymbol{s}_{-ik^*})(\{j\})\ (j = 1, 2, ..., n)$ and NC. If $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ is the Nash equilibrium solution of the biform game $(S_1, S_2, ..., S_m; V)$, then $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*})$ is an effective strategy situation.

Corollary 3. Assume that the characteristic function of the biform game $(S_1, S_2, ..., S_m; V)$ satisfies $V(S_k)(\{j\}) = V(r_i, \boldsymbol{s}_{-ik^*})(\{j\})\ (j = 1, 2, ..., n)$ and NC. If $S_{k^*} = (s_{1k^*}, s_{2k^*}, ..., s_{nk^*})$ is an effective strategy situation, then $\{S_{k^*}; (SCIS_1(V(S_{k^*})), SCIS_2(V(S_{k^*})), ..., SCIS_n(V(S_{k^*})))\}$ is the Nash equilibrium solution of the biform game $(S_1, S_2, ..., S_m; V)$.

3.3. Solution Steps

From the above discussion, the solution steps of the mining pool biform game model are summarized as follows:

Step 1. (the non-cooperation stage): All the miners in the mining pool choose strategies and execute strategy combinations to form strategy situation $S_k\ (k = 1, 2, ..., m)$.

Step 2. (the cooperation stage): For any strategy situation $S_k\ (k = 1, 2, ..., m)$ formed by the miners, we construct the cooperative games. Simultaneously, according to Eq. (1), we construct the characteristic functions.

Step 3. (the solution of cooperation stage): We calculate the semi-CIS $SCIS_i(V(S_k))$ of each miner $i\ (i = 1, 2, ..., n)$ in the situation $S_k\ (k = 1, 2, ..., m)$ by using Eq. (2).

Step 4. (the solution of non-cooperation stage): The semi-CIS $SCIS_i(V(S_k))$ value obtained in the third step is used as payment vector value of each miner under the strategy situation S_k in the non-cooperation stage. Then we construct the non-cooperative game and solve the Nash equilibrium solutions. That is to analyze and solve the Nash equilibrium solutions in the non-cooperative game.

According to the pure strategy Nash equilibrium solutions in the fourth step, we can determine the strategy choice of the entire mining pool. That is to say, we can get a mining pool strategy to maximize the profits (or utilities) of each miner and the entire mining pool.

4. A NUMERICAL EXAMPLE

Let us consider a simple example: there are three miners (i.e., players) 1, 2, and 3 in a mining pool. In order to obtain high profit, the miners 1, 2, and 3 have to make strategy choices. Stated as earlier, they have two strategies to choose: the malicious strategy (remark 0) and the honest strategy (remark 1). We set system parameters as follows: $R + \theta s = 15$, $\omega = 200$, and $\gamma = 0.3$. The miners' computing powers are $\omega_1 = 3$, $\omega_2 = 5$, and $\omega_3 = 2$, respectively. So the entire computing power of the mining pool is $\omega_G = 10$. It is easily to get $\omega_l = min\{\omega_i\} = 2$. And we set $\lambda = 0.01 \leq (1-\gamma)[(R+\theta s)\omega_l/(\omega\omega_G)] = 0.0105$. The selfish levels of the miners are $\alpha_1 = 0.8$, $\alpha_2 = 0.2$ and $\alpha_3 = 0.6$, respectively.

4.1. Solving the Cooperative Game Stage

The above example is related both strategy choices (non-cooperation stage) and mutual cooperation (cooperation stage) among the miners 1, 2, and 3. Consequently, it can be seen as a biform game problem. We can use the solution steps in Section 3.3 to solve this problem.

Stated as earlier, the strategy situations formed by the miners 1, 2, and 3 are shown in Table 1. According to Eq. (1) and Table 1, we calculate the coalitions profits (or utilities) in every strategy situation as shown in Table 3 (This article only lists the profit values of the grand coalition and the individual miner coalition). Remark: When the calculation result is negative, we take 0.

4.2. Solving the Non-Cooperative Game Stage

According to Eq. (2), we calculate the semi-CIS value $SCIS_i(V(S_k))$ of each miner $i\ (i = 1, 2, ..., n)$ as shown in Table 4. We can see all the miners' profits are zero if all of them choose the malicious strategy.

Then taking the semi-CIS values in Table 4 as the corresponding profit values of the miners in various strategy situations. For each strategy situation, we calculate the sum of the profit values of all the miners, i.e., calculating the total profit value in the situation, which is expressed as

$$SCIS(V(S_k))(N) = \sum_{i \in N} SCIS_i(V(S_k))(N).$$

The calculation results are shown in Table 5.

In the following, we take the maximum value of $SCIS(V(S_k))(N)$, i.e., $\max\{SCIS(V(S_k))(N)\}$. According to Theorem 4 and Theorem 5, we analyze whether the strategy corresponding to the maximum value is a pure strategy Nash equilibrium solution. Then we analyze the sub-maximum. We repeat the above steps until there are no other pure strategy Nash equilibrium solutions. Specifically, we firstly sequence the total profit values $SCIS(V(S_k))(N)$, $(k^* \in \{1, 2, ..., m\})$ for all situations according to Tables 3 and 4, then we take the maximum value $\max\limits_{1 \leq k \leq 8}\{SCIS(V(S_k))(N)\}$. The sequence of the total profit values is shown as follows: $SCIS(V(S_8)) = 0.6712 > SCIS(V(S_6)) = 0.5782 > ... > SCIS(V(S_3)) = 0.0166 > SCIS(V(S_1)) = 0$.

And the maximum value is $\max\limits_{1 \leq k \leq 8}\{SCIS(V(S_k))(N)\} = SCIS(V(S_8)) = 0.6712$, i.e., the profit of the entire mining pool reaches the maximum value when all the miners choose the honest strategy to form the strategy situation $S_8 = (1, 1, 1)$. And the corresponding semi-CIS value

Table 3 The coalitions profits in every strategy situation.

Strategies		Miner 3			
		0		1	
		Miner 2		Miner 2	
		0	1	0	1
Miner 1	0	$\mathbf{v}(S_1)(1,2,3)=0$ $\mathbf{v}(S_1)(1)=0$ $\mathbf{v}(S_1)(2)=0$ $\mathbf{v}(S_1)(3)=0$	$\mathbf{v}(S_2)(1,2,3)=0.4225$ $\mathbf{v}(S_2)(1)=0$ $\mathbf{v}(S_2)(2)=0.1375$ $\mathbf{v}(S_2)(3)=0$	$\mathbf{v}(S_3)(1,2,3)=0.0145$ $\mathbf{v}(S_3)(1)=0$ $\mathbf{v}(S_3)(2)=0.0019$ $\mathbf{v}(S_3)(3)=0.01$	$\mathbf{v}(S_4)(1,2,3)=0.5135$ $\mathbf{v}(S_4)(1)=0$ $\mathbf{v}(S_4)(2)=0.1375$ $\mathbf{v}(S_4)(3)=0.01$
	1	$\mathbf{v}(S_5)(1,2,3)=0.3315$ $\mathbf{v}(S_5)(1)=0.0375$ $\mathbf{v}(S_5)(2)=0.0019$ $\mathbf{v}(S_5)(3)=0$	$\mathbf{v}(S_6)(1,2,3)=0.559$ $\mathbf{v}(S_6)(1)=0.0375$ $\mathbf{v}(S_6)(2)=0.1375$ $\mathbf{v}(S_6)(3)=0$	$\mathbf{v}(S_7)(1,2,3)=0.4225$ $\mathbf{v}(S_7)(1)=0.0375$ $\mathbf{v}(S_7)(2)=0.0019$ $\mathbf{v}(S_7)(3)=0.01$	$\mathbf{v}(S_8)(1,2,3)=0.65$ $\mathbf{v}(S_8)(1)=0.0375$ $\mathbf{v}(S_8)(2)=0.1375$ $\mathbf{v}(S_8)(3)=0.01$

Table 4 The coalitions profits in every strategy situation.

Strategies		Miner 3			
		0		1	
		Miner 2		Miner 2	
		0	1	0	1
Miner 1	0	(0, 0, 0)	(0.1317, 0.1683, 0.1317)	(0.0027, 0.0032, 0.0107)	(0.16, 0.1967, 0.168)
	1	(0.1404, 0.1009, 0.1004)	(0.2072, 0.2038, 0.1672)	(0.1687, 0.1292, 0.1367)	(0.2355, 0.2322, 0.2035)

Table 5 The total profit values in each strategy situation (semi-CIS values).

Strategies		Miner 3			
		0		1	
		Miner 2		Miner 2	
		0	1	0	1
Miner 1	0	$SCIS\left(V\left(S_1\right)\right)(N)=0$	$SCIS\left(V\left(S_2\right)\right)(N)=0.4317$	$SCIS\left(V\left(S_3\right)\right)(N)=0.0166$	$SCIS\left(V\left(S_4\right)\right)(N)=0.5247$
	1	$SCIS\left(V\left(S_5\right)\right)(N)=0.3417$	$SCIS\left(V\left(S_6\right)\right)(N)=0.5782$	$SCIS\left(V\left(S_7\right)\right)(N)=0.4346$	$SCIS\left(V\left(S_8\right)\right)(N)=0.6712$

is $(SCIS_1(V(S_8)), SCIS_2(V(S_8)), SCIS_3(V(S_8))) = (0.2355, 0.2322, 0.2035)$.

Thereby, the solution of the biform game is $\{S_8; (SCIS_1(V(S_8)), SCIS_2(V(S_8)), SCIS_3(V(S_8)))\} = \{(1,1,1); (0.2355, 0.2322, 0.2035)\}$.

Further analysis can obtain that $V(S_8)(N) \geq V\left(r_i, \boldsymbol{s}_{-ik^*,8}\right)(N)\,(i=1,2,3)$, which is consistent with the conclusion of Theorem 4. That is, when a player in the game changes its strategy and the other players do not change their strategies, its profit value will be less than that in the current strategy situation. Hence, the strategy situation $S_8 = (1,1,1)$ is the pure strategy Nash equilibrium solution of the non-cooperation stage in this biform game model.

Analogously, the corresponding strategy situation of submaximum value $SCIS(V(S_6)) = 0.5782$ is $S_6 = (1,1,0)$, and the corresponding solution of the biform game is $\{S_6; (SCIS_1(V(S_6)), SCIS_2(V(S_6)), SCIS_3(V(S_6)))\} = \{(1,1,0); (0.2072, 0.2038, 0.1672)\}$.

Because $V(S_8)(N) \geq V(S_6)(N)$, the strategy situation $S_6 = (1,1,0)$ does not satisfy Theorem 4. It is not the pure strategy Nash equilibrium solution of the non-cooperation in this biform game model. Repeat the above steps until all pure strategy Nash equilibrium solutions are obtained.

Through the above analysis, we can conclude that $S_8 = (1,1,1)$ is the only pure strategy Nash equilibrium of the biform game. So the mining pool and each miner get the optimal profits when all the miners choose the honest strategy. The corresponding Nash equilibrium value is (0.2355, 0.2322, 0.2035). That is, the mining pool biform game model solution is $\{S_8; (SCIS_1(V(S_8)), SCIS_2(V(S_8)), SCIS_3(V(S_8)))\} = \{(1,1,1); (0.2355, 0.2322, 0.2035)\}$

5. CONCLUSIONS

In order to prevent miners from initiating block withholding attack, this paper models the mining process as a biform game, wherein the miners might choose whether to attack or not. And we set constraints to maintain the voluntary honest behavior of miners during the cooperation stage. Though analyzing and researching the numerical example, we can conclude that the biform game can well solve the miners strategy choices and benefits distribution problems, and can prevent the block withholding attack effectively. Moreover, the biform game can make up for the shortcomings of using the single cooperative game or non-cooperative game method. Specifically, it makes up the deficiency of non-cooperative game that the players only care about strategy design without considering the payoff distribution of coalitions. Simultaneously, it also remedy the cooperative game only analyze the coalition

formation and its payoff distribution without taking into account strategy design and selection. Besides, the solutions of the biform game must be the pure strategy Nash equilibrium solution, so it can better guide the miners strategy choice.

In this paper, we propose the semi-CIS value, which can guarantee the existence and uniqueness of the solution in the cooperation stage, to solve the payoff values of cooperative game. And the existence conditions of the solution of the biform game are given. In summary, this paper not only provides a new solution to the miners' action of initiating block withholding attack problem, but also enriches the application research of the biform game method.

This study only considers the influence of computing power on the profit of the mining pool, but there are many other factors to affect the profit of the mining pool such as mining machine, mining pool site. And this study is only applicable to the case that the number of miners in the mining pool is constant. Not considering the dynamic change in the number of miners in the mining pool. So we will carry out the above researches in the future.

CONFLICT OF INTEREST

Firstly, there is no potential conflict of interest.

AUTHORS' CONTRIBUTIONS

Xiao-Li Du developed the model, performed the analysis, and wrote the paper. Deng-Feng Li conceived the presented idea, and provided critical feedback and helped shape the research, analysis, and manuscript. Kai-Rong Liang was responsible for collecting the data and writing the first draft.

Funding Statement

Lastly, the funding statement is as follow: The authors would like to acknowledge the financial support from the National Natural Science Foundation of China (Grant Nos. 71231003).

ACKNOWLEDGMENTS

The authors would like to acknowledge the financial support from the National Natural Science Foundation of China (Grant ♯: 71231003).

REFERENCES

[1] A. Sarker, S. Wuthier, S.Y. Chang, Short paper: anti-withholding reward system to secure blockchain mining pools, in Proceedings - 2019 Crypto Valley Conference on Blockchain Technology, IEEE, Rotkreuz, 2019, pp. 43–46.

[2] D.K. Tosh, S. Shetty, X.P. Liang, C.A. Kamhoua, K.A. Kwiat, L. Njilla, Security implications of blockchain cloud with analysis of block withholding attack, in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 7973732, IEEE, Madrid, 2017, pp. 458–467.

[3] S. Siamak and P.B. Maria, Brief announcement: ZeroBlock: timestamp-free prevention of block-withholding attack in bitcoin, in: P. Spirakis, P. Tsigas (Eds.), SSS 2017: Stabilization, Safety, and Security of Distributed Systems, Springer, Cham, 2017, 356–360.

[4] S.Y. Chang, Y. Park, Silent timestamping for blockchain mining pool security, in 2019 International Conference on Computing, Networking and Communications, ICNC, Honolulu, 2019.

[5] A.T. Haghighat, M. Shajari, Block withholding game among bitcoin mining pools, Future Gener. Comput. Syst. Int. J. Esci. 97 (2019), 482–491.

[6] Y. Wang, C.B. Tang, F.L. Lin, Z.L. Zheng, Z.Y. Chen, Formation Games of Reliable Networks, Pool strategies selection in PoW-based blockchain networks: game-theoretic analysis, IEEE Access. 7 (2019), 8427–8436.

[7] C.B. Tang, C.J. Li, X.H. Yu, Z.L. Zheng, Z.Y. Chen, Cooperative mining in blockchain networks with zero-determinant strategies, IEEE Trans. Cybern. (2019), 1–6. https://ieeexplore.ieee.org/document/8720232.

[8] Q. Hu, S.L. Wang, X.Z. Cheng, A game theoretic analysis on block withholding attacks using the zero-determinant strategy, in Proceedings of the International Symposium on Quality of Service, (IWQoS 2019), Ariona, 2019.

[9] D. Wu, X.D. Liu, X.B. Yan, R. Peng, G. Li, Equilibrium analysis of bitcoin block withholding attack: a generalized model, Reliab. Eng. Syst. Saf. 185 (2019), 318–328.

[10] S. Bag, S. Ruj, K. Sakurai, Bitcoin block withholding attack: analysis and mitigation, IEEE Trans. Inf. Forensics Secur. 12 (2017), 1967–1978.

[11] A. Brandenburger, H. Stuart, Biform games, Manage. Sci. 53 (2007), 537–549.

[12] M.D. Ryall, O. Sorenson, Brokers and competitive advantage, Manage. Sci. 53 (2007), 566–583.

[13] L. Gui, A. Atasu, Ö. Ergun, L.B. Toktay, Design incentives under collective extended producer responsibility: a network perspective, Manage. Sci. 64 (2018), 5083–5104.

[14] S. Mahioub, J.C. Hennet, Manufacturers' coalition under a price elastic market - a quadratic production game approach, Int. J. Prod. Res. 52 (2014), 3568–3582.

[15] E. Feess, J.H. Thun, Surplus division and investment incentives in supply chains: a biform-game analysis, Eur. J. Oper. Res. 234 (2014), 763–773.

[16] S. Kim, Reverse-biform game based resource sharing scheme for wireless body area networks, Int. J. Ad Hoc Ubiq. Comput. 31 (2019), 219– 229.

[17] D.S. Hou, P.F. Sun, G.J. Xu, Compromise for the complaint: an optimization approach to the ENSC value and the CIS value, J. Oper. Res. Soc. 69 (2016), 571–579.

[18] G.J. Xu, H. Dai, H.B. Shi, Axiomatizations and a noncooperative interpretation of the α-CIS value, Asia Pac. J. Oper. Res. 32 1– 15 (2015), 1550031.