Cooperation Mechanism in Blockchain by Evolutionary Game Theory

Jinxin Zhang and Meng Wu

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Correspondence should be addressed to Meng Wu; wum@njupt.edu.cn

Received 9 September 2021; Accepted 20 October 2021; Published 8 November 2021

Copyright © 2021 Jinxin Zhang and Meng Wu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the blockchain network, to get rewards in the blockchain, blockchain participants pay for various forms of competition such as computing power, stakes, and other resources. Because of the need to pay a certain cost, individual participants cooperate to maintain the long-term stability of the blockchain jointly. In the course of such competition, the game between each other has appeared invisibly. To better understand the blockchain design of cooperation mechanisms, in this paper, we constructed a game framework between participants with different willingness, using evolutionary game theory, and complex network games. We analyzed how the behavior of participants potentially develops with cost and payoff. We consider the expected benefits of participants for the normal growth of the blockchain as the major factor. Considering the behavior of malicious betrayers, the blockchain needs to be maintained in the early stage. Numerical simulation supports our analysis.

1. Introduction

The public blockchain is a peer-to-peer (P2P) network that is used to build a decentralized ledger and can be trusted to achieve autonomy without third-party supervision. The most well known of all blockchains is Bitcoin, in which the Nakamoto consensus protocol [1] creatively integrates a variety of mechanisms and technologies, laying the foundation for the subsequent development of the blockchain. Blockchain technology has the characteristics of decentralization, traceability, non-tampering, programmability, and collective maintenance.

Blockchain is a time-ordered one-in-one-out directed graph, interconnected to form a chain structure that uses cryptography to ensure that the distributed ledger is tamper-evident and unforgeable. In a broad sense, blockchain technology is a new distributed infrastructure and computing paradigm. It uses a blockchain data structure to store data, decentralized node consensus algorithms to generate and verify data, cryptography to secure data transmission and access, and smart contracts composed of automated scripting code to use data.

Besides applying some sophisticated technologies, the blockchain also considers some mechanisms. In the blockchain represented by Bitcoin, the entire nodes (block miners) are economically encouraged to abide by the “longest chain policy” to preserve the stability of the blockchain. Most blockchains follow this policy. The block bookkeeper packs any set of verified transactions into a data structure, announced a candidate “block,” and broadcasts it to the entire network. Each blockchain participant consistently uses the longest chain as its local blockchain copy. This design can ensure that we can write the new blocks with the most resources into the chain in time.

Many blockchains also used bitcoin’s incentive mechanism. It comprises two parts: effort and reward.
(i) **Effort.** The process of solving intensive problems makes Sybil attacks [2] economically unbearable.

(ii) **Reward.** The reward given to the new block producer (miner) will be released after the network admits the block it publishes.

Taking Bitcoin as an example, the hash puzzle-solving process is regarded as a computing power competition among miners. After investing in a certain amount of effort, the miners will get two types of rewards during the mining process: new currency rewards for creating new blocks and transaction fees included in the block. To get these rewards, miners are vying to complete a mathematical puzzle based on a cryptographic hash algorithm, which requires powerful computing power. In addition, each transaction may include a transaction fee. Miners who successfully “dig out” a new block during the mining process can receive “tips” for all transactions recorded in the block. The competition of this algorithm and the mechanism by which the winner has the all right to record transactions on the blockchain provide the safety of Bitcoin. Blockchain is a competitive platform for users. The anonymity of its participants and the transparency of network information create innate conditions for pursuing a balanced game. And the periodic expansion of new blocks in the blockchain provides an appropriate arena for repeated games.

Some scholars have applied game models to blockchain issues. How many transactions a new block contains is the miner’s choice. Houy [3] defined the Bitcoin mining game between miners, assuming that the number of transactions in a block results from the game, and studied the Nash equilibrium of the game. From the perspective of game theory, Schrijvers et al. [4] defined the mining pool payment function in a single mine pool and analyzed whether several mining pool strategies meet the requirements of incentive compatibility, proportional payment, and budget balance. Eyal discussed the attack between the two mining pools [5], there is a contradiction between individual rationality and collective rationality between the pools, which is like the tragedy game of the commons. He believes that the interception attack reduces the computing power of the entire network.

Security issues in the blockchain have always been the concentrate of attention. 51% attack, selfish mining attack [6], and other threats always exist. The focus of this article is the impact of the strategic choice of each blockchain participant on the cooperation mechanism. We consider individual miners have bounded rationality and will adopt specific participation strategies in the blockchain. We model the strategy choice in the network as an evolutionary game and study the evolutionary stability of the dynamics of strategy selection.

The contributions of this paper are threefold. (1) We formulate the cooperative behavior on the blockchain. (2) We use evolutionary game theory to analyze how the participants of the blockchain change their strategies and their incentives. (3) We also analyzed the influence of network structure on cooperative behavior on the blockchain.

We organized this paper as follows. In Section 2, we review the background on security issues in the blockchain and evolutionary game theory. We formalize the new block generation right game and analyze it in Section 3. In Section 4, we assign values to the parameters in the model and conduct simulations and discuss the results. Finally, we conclude with future directions in Section 5.

## 2. Background

### 2.1. The Relationship between Cooperation, Trust, and Security

Cooperation, trust, and security are three concepts that are connected with each other and have their emphasis.

Different security scenarios, relationship types, and social interactions within the system require different levels of trust. Trust depends on the restraint of the interacting parties, which is usually determined by agreement in the system. Since trust involves both risks and benefits, the need for trust is different for cooperation. Stomppka [7] believes that the simplest definition of trust is the gamble of believing in the future actions of others. Gambetta [8] emphasized that trust required depends on the strength of the mechanism that determines cooperative decision-making, and it also depends on the social context in which we decide and treats trust as “a result of cooperation.”

It does not base the basis of cooperation on pure trust, but on the continuity of the relationship. Axelrod and Hamilton [9] believe that, in the long run, whether the conditions for the establishment of a stable cooperation model between the two parties are mature is more important than whether they trust each other. In order for cooperation to be stable, there must be a large enough incentive in the future. It requires that the participants in the system have a large enough chance to meet again, and the meaning of their encounter again cannot be discounted too much.

Lamsal believes that trust and security are tightly coupled [10]. There are various ways to provide security services. However, encryption is one of the most extensive and effective ways to provide these services. But the management of cryptographic keys becomes a problem. The fundamental problem that any key management system is trying to solve: Is the key trusted?

Trust and security go hand in hand, and trustworthiness is the foundation of security. A trusted mechanism cannot accomplish any security function alone but can be implemented in various systems and work with the security mechanism of the system to play the role of reinforcing and managing security. But traditional security measures cannot really cover the smart environment, so trust is important. “6G White Paper: Research Challenges for Trust, Security and Privacy” [11] pointed out that the 6G network must support embedded trust for an increased level of information security in 6G. Trust modeling, trust policies, and trust mechanisms need to be defined.

In the modern network environment, users do not feel what kind of information has been collected, and they do not know where and who uses this information. With the gradual popularity of such application scenarios, the concept of trust has recently approached the concept of security and is closer to the needs of users. As the cooperative relationship between the participants in the network advances, the trust relationship is established unconsciously.
2.2. Security Issues in Blockchain. Blockchain uses some mature cryptographic principles and consensus mechanisms based on distributed ledger technology to realize trusted interaction without the intervention of a third party in a distributed environment. The improvement of system efficiency and cost reduction brought by blockchain provides new methods for economic and social development and various industries. Blockchain can build trust in a low-cost way. Blockchain has developed rapidly recently, and scholars have tried to use blockchain in fields such as medical care [12], edge computing [13], and the Internet of Things [14, 15].

These application areas involve the following features of blockchain technology.

(i) Decentralization. The blockchain network is based on a peer-to-peer (P2P) network to create information broadcasts, and the failure of a single node has no global impact.

(ii) Untamperable. All nodes maintain the ledger in the blockchain, and the consensus mechanism ensures that most nodes allow the ledger and provides a strong correlation between data blocks with a hash function, and the data on the chain are open to the entire network, and the data are verifiable and traceable.

(iii) Anonymity. Cryptography and other technologies separate the user’s real identity from the network identity so that the user’s identity can be protected and establish a foundation of trust at the same time.

In a blockchain network without third-party supervision, the essence of security is the confrontation between honest participants and malicious betrayers. Traditional network security threats will also exist in P2P network; using identity authentication, intrusion detection, traffic monitoring, etc., plays a significant role in network security protection. However, defense often lags attacks, and it is intractable to respond to more complex attacks and defenses in the network promptly. With the risk of more complex attacks, it is also a major challenge to coordinate the selection of defense strategies and generate attack responses before the attackers have caused severe losses. Besides the traditional security, the special scenario of the blockchain network takes unique challenges to the network security. This is because traditional data-based network security research methods are problematic to handle with blockchain network attacks that have real monetary benefits.

The blockchain suffers the following security threats:

(i) 51% Attack. The 51% attack is an attack method that uses computing power as a competitive condition and controls the advantage of computing power to cancel payment transactions that have occurred. Blockchain networks such as Bitcoin have encryption security because of decentralization. After most nodes on the Bitcoin network agree, the public ledger is credible. However, if a single entity or team can control over 50% of the hash rate, then they can change the state of the blockchain. It can get the random number needed to mine the block faster than others and decide the packaged transaction and affect the effectiveness of the block. After launching the attack, the attacker will continuously destroy the value of a cryptocurrency by implementing double-spending or posting various fraudulent transfers on the chain.

(ii) Selfish Mining. A selfish mining attack is a method against Bitcoin mining and the incentive mechanism. Its purpose is not to destroy the operating mechanism of Bitcoin, but to pursue additional rewards and make honest miners perform invalid calculations.

In short, the core idea of a selfish mining attack is that malicious mining pools deliberately delay publishing new blocks worked out by them, and create a private branch under their control, making the chain to fork. Honest miners continue to mine based on public branches, while malicious mining pools mine based on private branches controlled by them. If the malicious mining pool calculates more blocks, the length of the private branch they control is naturally ahead of the public branch. The malicious mining pool chooses not to rush to publish these new blocks and strives to further increase the mining revenue. However, because of the limitation of the computing power of the malicious mining pool, the length advantage of the private branch will not be maintained consistently. When the public branch is close to the length of the private branch, the malicious mining pool will announce the branch generated by itself to replace the legal one and take the reward of these new blocks.

(iii) Eclipse Attacks. The method of eclipse attacks [16] is different from 51% attack. They attack specific nodes or node clusters so that the network appears “partitioned” to achieve double-spending and other purposes. Due to network spare capacity and computing power distribution limitations, the blockchain usually limits the upper limit of a single node that can receive information and actively link to other nodes. The concentrate of an eclipse attack is to start with the information of the nodes linked to and received. If the node receiving information and the externally linked nodes are all controlled by malicious nodes, it is equivalent that the malicious nodes isolate and control the received information to the target node. Here, it is called the node that suffered an “eclipse attack.” If the malicious nodes can control more nodes and launch an eclipse attack on more normal nodes, then the malicious nodes will split the blockchain network into two distinct partitions, just like a fork.

2.3. Application of Evolutionary Game Theory in Blockchain. In game theory, players can adopt several strategies, have a certain influence on other players, and get a certain payoff in the interaction. Game theory is the study of rational choice of strategies between individuals to pursue the maximization of their interests. The core concept is Nash
equilibrium. Daskalakis et al. [17] conclude that it is almost impossible to find Nash equilibrium on a large scale in action-graph games. They proved it belongs to a subset of the NP problem. But when the participants are anonymous, they need only polynomial time to approach the Nash equilibrium.

The evolutionary game theory concentrates on how individuals with bounded rationality can continuously optimize their payoffs by comparing in the repeated game. Similar to the concept of fitness in the evolution of nature, players with a high payoff are more likely to take part in the next round of the game, while a play with a low payoff is more likely to be eliminated. Eventually, a particular strategy will reach equilibrium in the system.

The blockchain is a natural testing ground in this respect because of the following characteristics:

1. Based on the decentralized P2P communication method, information symmetry becomes workable. In the blockchain network, all individuals share the same database, and all information releases appear as broadcast. Then, not only are the two parties in the transaction holding information, but all communicating parties have corresponding information. This has completely changed the limitations of information asymmetry between the two parties and created conditions for joint decision-making.

2. The status of participants in the blockchain is equal. Besides the alliance chain, which is between the public chain and the private chain, the rights and status of the nodes in an individual blockchain are equal. It enhances the autonomy of decision-making. In the game, the inequality of social status is prone to cause a party to have the dominant advantage, making the result more predisposed to the dominant party. The blockchain has changed this state and created a nearly free environment, making it easier to analyze the results in a rational decision-making manner. With the blessing of blockchain technology, both parties to the transaction have complete transaction data, and each transaction subject can make independent decisions based on their knowledge, and there is almost no distinction in transaction rights.

3. Cryptography provides a credible environment. All participants and their information on the blockchain are digital. On the premise that it does not compromise encryption technology, transaction data is irreversible and cannot be denied. Participants in the transaction process are more prone to trust each other.

4. Generating new blocks with no curb on the rounds creates conditions for repeated games. We can consider the processing of each new block as a repeated game, and participants do not demand to reveal their private keys and remain anonymous. As the chain continues to grow, it reaches the Nash equilibrium.

In a complex network environment, players do not have sufficient ability to get global information, nor have enough ability to choose the best strategy to maximize their profits. This condition of blockchain shows that participants are bounded to rationality in the strategy selection process.

There are two types of behaviors in the system: cooperation and defection. Cooperation refers to the behavior of paying a definite cost to benefit the opponent, but defection is to get benefits from other players. According to the law of survival of the fittest, high payoff players will eliminate low payoff ones.

There will be group selection [18] among players. A group can contain several players, and the players within the group are cooperative, while the groups are competing. The contact relationship of blockchain participants also needs to be considered, which can be represented by the network. In the network, the node means a player, and the edge between nodes serves as the game relationship between players. In each round of the game, players interact according to the game model and update their strategies according to payoffs.

From a security perspective, purely technical cannot completely resolve the security threats of the blockchain system, and the design of the mechanism brings a new perspective to answer security issues.

3. The Evolutionary Game of Blockchain Security

The reason attack in the blockchain is hard to raise is not that these participants have noble morals, but that they have calculated that the benefits of honest participation are higher than malicious attacks. That is why they maintain the blockchain system instead of destroying it. Not only suffering 51% attacks, but the blockchain must also be able to resist a variety of attacks. While using various security technologies, it is necessary to construct an excellent mechanism. For example, in the process of evolution of the blockchain, there are competition mechanisms [19, 20] and voting mechanisms [21], etc. These mechanisms drive the blockchain more secure. Blockchain is a consensus system that pursues Nash equilibrium and the Nash equilibrium point of a blockchain system with an efficient mechanism design can approach the optimal ideal state. This is also a significant reason to treat blockchain as a revolutionary technology.

When the miners successfully dig a block, they become the block producer in this round. They can charge a fee for the included transactions. They can also get additional economic rewards for new block. This is an incentive for miners. With the uninterrupted generation of new blocks, each participant continuously improves its game strategy by learning the experience of the winners and forms a fresh offensive and defensive situation. Motivated by the continuous improvement of the game strategy of the blockchain participants, a developing defense-attack system of the blockchain has finally been established.

3.1. Description and Assumptions of the Model. In the blockchain system, different participants have distinct preferences. To facilitate the model, we arrange all miners
into two groups. Group A presents an inclination for cooperation, while group B is more selfish. In the evolutionary game, both groups A and B can only have access to insufficient information with bounded rationality. And they both imitate the strategies they would consider most helpful and improve the strategies they have worked in previous. Both groups will constantly adjust their strategies to maximize their payoffs.

The strategies of the two sides of the game include the “cooperation” strategy of observing the consensus mechanism and the “defection” strategy of not observing the consensus mechanism. The following are the assumptions and parameter descriptions in the model.

Define the cooperation cost of participants in group A as $C_a$ and the cost of participants in group B as $C_b$. The distinction between the two groups is that group A tends to abide by the rules and gets payoffs on the blockchain honestly; with more computing power and other resources, participants of group B are more prone to invest in hostile costs to get payoffs on the blockchain. We define the total revenue brought by each round of the game as $R$, which will be distributed to two groups of participants after each round. When a serious malicious attack occurs in the blockchain, participants will suspect the sustainability of the blockchain system, and the revenue $R$ cannot be maintained. To establish the long-term validity and rationality of the blockchain, the model satisfies the following conditions: $C_a > C_b, R > C_a + C_b$.

Considering that no matter what participation means, the participants chosen, even adopt some attacks, each round of block generation game will gain certain benefits as long as the blockchain can continue to run. However, this type of payoff has distinct expectations for various participants. Participants in group A can get mining rewards and commission income in the forthcoming. This type of expected payoff is defined as $K_a$, and group B will have hope it can control the blockchain to get illegal revenue, and we define this kind of expected revenue as $K_b$.

In order to reduce the occurrence of malicious situations, the blockchain system adopts some punitive measures, adding some regulations to the consensus mechanism, such as delaying the issuance of mining rewards and collecting deposits. We use $P$ to represent this kind of punishment.

### 3.2. Model Analysis

Based on the assumptions and parameters in the previous section, this section establishes a payment matrix between blockchain participants. Players adopt various strategies, get the payoffs, and establish a dynamic system. We show the strategy matrix in Table 1.

We use $E^h_{ab}, E^m_{ab}$ to denote the payoffs of participants in group A using different strategies (honest cooperation, malicious defection), and the payoffs of participants in group B are $E^h_{ba}, E^m_{ba}$.

\[
E^h_a = y(K_a + \lambda R - C_a) + (1 - y)(K_a - C_a),
\]
\[
E^m_a = y(K_a - C_a - P) + (1 - y)(K_a - P),
\]
\[
E^h_b = x(K_b + (1 - \lambda)R - C_b) + (1 - x)(K_b - C_b - P),
\]
\[
E^m_b = x(K_b - C_b) + (1 - x)(K_b - P).
\]

The average expected benefits of the two groups are

\[
E_a = xE^h_a + (1 - x)E^m_a,
\]
\[
E_b = yE^h_b + (1 - y)E^m_b.
\]

Therefore, the dynamic equations for participants to choose cooperation strategies can be expressed as $F(x), F(y)$. Assume that the growth rate of the proportion of participants in various groups is equal to its benefits minus the average expected benefits of this group of participants.

\[
F(x) = \frac{dx}{dt} = \frac{x}{x + y}(E^h_a - E_a),
\]
\[
F(y) = \frac{dy}{dt} = \frac{y}{x + y}(E^m_b - E_b).
\]

Unlike classical one-shot games, in the blockchain system, participants can take part in the game many times, and each block produced is regarded as a fresh round. Participants may shift their strategies. Malicious participants may attack or persuade honest participants to change their strategies in the next game. To investigate the changing state of participants, we employ evolutionary games in our analysis.

Assume that all blockchain participants have designated a specific strategy at the genesis round. All participants are honest or malicious, and they stay in the blockchain environment in a certain proportion. After several rounds of games, we examine the changes in the population.

In the evolutionary game, the evolutionary stable strategy (ESS) is a strategy that other strategies cannot invade. The case with punishment has a strong ESS because, according to the loss aversion theory [22], punishment can influence decision-making more than not getting incentives.

### 3.3. Blockchain Evolutionary Game in the Complex Network Environment

Game model, network structure, and evolution rules are the three important factors of network evolution. Blockchain is based on a peer-to-peer network, which guarantees the fairness of the status of nodes to the greatest extent. In the classic evolutionary game theory, the contact relationship between players is uniform. However, the relationship between participants in the blockchain is completely random. Therefore, the actual network factor is also an important part to be considered. The network can describe the connection relationship between blockchain participants. Each node
represents a participant, and the edges between nodes represent the communication relationship between participants. In each round of the blockchain generation process, participants adopt evolution rules to update the game strategy.

In the small-world network, it is easier for collaborators to unite on the random network to form a large cooperative cluster, which promotes the emergence of cooperative behavior on the random network [23]. The emergence of cooperation in BA scale-free networks has emerged in many types of games, and the collaborators occupy the dominant position in the network [24]. In the BA scale-free network, the central nodes exist as stubborn collaborators. These pure collaborators can effectively resist the attacks of malicious betrayers by forming an interconnected subnet.

In the blockchain network, various participants are pursuing payoffs, but the methods used are distinct. From the perspective of blockchain security, besides paying attention to collaborators, the behavior of betrayers needs more attention. Each coin has two sides. The influence of the network structure on cooperative behavior also has a corresponding influence on the betrayers.

Except for some alliance chains and private chains, most of the blockchains have incentive mechanisms to adjust their expectations for future benefits. The blockchain system encourages participants to work actively, so that there are enough nodes in the system to ensure the normal operation of the system. Incentive theory ensures that a rational participant can continue to work honestly. If malicious participants are in a helpful position, blockchain will not reward them. Therefore, the best strategy for a rational blockchain participant is to maintain honest cooperation in the blockchain.

Distributed individuals maintaining this behavior will not pose a serious threat to the system, but malicious players contact each other to form a community structure in the network, which may pose a threat to the system. The mechanism design of the blockchain needs to ensure that rational behavior is honest. Therefore, if participants are dishonest, they will not be rewarded or even punished, so the expected future benefits will decrease. This has strong behavioral constraints on the bounded rationality assumption mentioned above and encourages miners to take part honestly in the blockchain.

In response to the above analysis, we designed corresponding simulation experiments. In the next paragraph, we will examine the development of cooperation in the blockchain from two different perspectives: the proportion of participants and the parameters in the game matrix.

### 4. Experimental Evaluation and Related Work

#### 4.1. Experimental Evaluation

We evaluate different profit situations through experiments to determine the changes in the proportion of honest collaborators and malicious participants in the population in the blockchain system under distinct game conditions. We ran experiments for the reward matrix of the case (Table 2).

Initially, 67% of group A were honest cooperators, and 20% of group B were malicious betrayers. Blue and red signify the proportions of validators with honest and malicious strategies, respectively. The Y-axis tracks the population proportions, and the X-axis tracks the generations (i.e., block rounds). As shown in Figure 1, we can notice that the honest strategy is an ESS.

We also run simulations by modifying the initial proportions of malicious participants. The initial proportions of malicious participants range from 0 to 33%. As shown in Figure 2, the proportion of malicious participants has shown a downward tendency.

In the simulation experiment, we discover that, although the honest strategy is ESS, it is a weak ESS when group B’s expected payoffs become higher, which is shown in Figure 3. The speculation is that when participants notice that there is a high expected payoff with defection, it will motivate them to flourish in a malicious direction.

The above experiment does not consider the influence of the network structure on the blockchain game and the frequency of cooperation. We use the parameters in Table 2 to design the game within the group A population in two typical complex networks in Figure 4. Figure 4(a) runs the WS small-
world model [25], and Figure 4(b) adopts the BA scale-free network model [26]. In the simulation, the NetworkX library of python is used. There are 1000 nodes in the WS network, and each node has 5 neighbors, and the probability of random reconnection is 0.3. There are 1000 nodes in the BA network, and it added 3 edges each time. The player follows the death-birth updating process. The simulation discloses that it takes quite lengthy rounds for honest collaborators to establish a trusting, cooperative relationship. This protracted process provides an opportunity for malicious behavior on the blockchain.

4.2. Related Work. In the research on the combination of blockchain and game theory, it mainly appears on the following topics: the game of mining behavior in the blockchain, security on the blockchain, and cryptocurrency and its applications.

In generating new blocks in the blockchain, there is a competitive mining process. This leads to a game between individuals. Some papers study the distribution of computing power [27] and the choice of forks [28]. With the continuous growth of miners, individual mining competition becomes more and more fierce. Therefore, miners spontaneously form mining alliances (mining pools). Some scholars conduct research on the choice of mining pools and the rewards in the mining pools [4, 29].

There are threats, such as selfish mining, 51% attacks, and denial of service (DoS) on the blockchain. Some papers start with the study of gaming behavior from the aspect of blockchain security. There is a game between the cost of an
attack on the blockchain and whether the system launches an attack and the strength of the attack [5, 30].

An important application of game theory is in the analysis of economic behavior, so a lot of research involves the game of economic behavior in the blockchain, for example, the choice between different cryptocurrencies [31], the choice of transactions when making a new block [32], and some payment behaviors involving actual transactions [33].

The article [34] focuses on the reward mechanism in the blockchain and uses evolutionary games to analyze how the behavior of participants develops with the reward mechanism. The authors also found that punishment plays a central role in maintaining the integrity of the blockchain. Compared with this article, in our blockchain game model, we found that future revenue expectations will affect the behavior of the blockchain. We also consider the influence of the network model on the cooperation mechanism in the blockchain.

5. Conclusion

We formulated the cooperation and defection behavioral game in the blockchain system. Using evolutionary game theory, we found the importance of reducing the profit expectations of malicious participants in maintaining the integrity of the ledger. When considering the influence of network factors, it takes a long time to establish a cooperative process within the blockchain. Thus, more attention needs to be paid to the security protection of the initial stage of the blockchain. These findings provide mechanism guidance for the security of the blockchain. A safe and reliable system should be considered from the most basic physical layer. We will start with the security and credibility requirements of the physical layer and design corresponding technologies and mechanisms, enhance our game model, and construct a stable blockchain mechanism.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study.

Acknowledgments

This work was funded by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX18_0903.

References

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” 2008, https://bitcoin.org/bitcoin.pdf.
[2] C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in Proceedings of the Annual International Cryptology Conference, pp. 139–147, Springer, Santa Barbara, CA, USA, 1992.
[3] N. Houy, “The bitcoin mining game,” Ledger, vol. 1, 2014.
[4] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, “Incentive compatibility of bitcoin mining pool reward functions,” in Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 477–498, Springer, Christ Church, Barbados, 2016.
[5] I. Eyal, "The miner’s dilemma," in Proceedings of the 2015 IEEE Symposium on Security and Privacy, pp. 89–103, IEEE, San Jose, CA, USA, 2015.

[6] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: generalizing selfish mining and combining with an eclipse attack," in Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroSeCS-P), pp. 305–320, IEEE, Saarbrücken, Germany, 2016.

[7] P. Sztompka, Trust: A Sociological Theory, Cambridge University Press, Cambridge, UK, 1999.

[8] D. Gambetta, "Can we trust trust," Trust: Making and breaking cooperative relations, vol. 13, pp. 213–237, 2000.

[9] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A multilevel selection," in Proceedings of the 20th Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 710–719, SIAM, New York, NY, USA, 2009.

[10] P. Lamsal, Understanding Trust and Security, Department of Computer Science, University of Helsinki, Helsinki, Finland, 2001.

[11] J. Zhang and M. Wu, "Blockchain use in IoT for privacy-preserving anti-pandemic home quarantine," Electronics, vol. 9, no. 10, p. 1746, 2020.

[12] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," Engineering, 2020.

[13] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: from theory to IoT applications and beyond," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8114–8154, 2019.

[14] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: a lightweight blockchain system for industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3571–3581, 2019.

[15] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin’s peer-to-peer network," in Proceedings of the 24th [USENIX] Security Symposium ([USENIX] Security 15), pp. 129–144, Santa Clara, CA, USA, 2015.

[16] C. Daskalakis, G. Schoenebeckt, G. Valiant, and P. Valiant, "On the complexity of Nash equilibria of action-graph games," in Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 710–719, SIAM, New York, NY, USA, 2009.

[17] A. Traulsen and M. A. Nowak, "Evolution of cooperation by multilevel selection," Proceedings of the National Academy of Sciences, vol. 103, no. 29, pp. 10952–10955, 2006.

[18] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity," ACM SIGMETRICS-Performance Evaluation Review, vol. 42, no. 3, pp. 34–37, 2014.

[19] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: a provably secure proof-of-stake blockchain protocol," in Proceedings of the Annual International Cryptology Conference, pp. 357–388, Springer International Publishing, Santa Barbara, CA, USA, 2017.

[20] I. Eyal, "The miner’s dilemma," in Proceedings of the 2015 IEEE Symposium on Security and Privacy, pp. 89–103, IEEE, San Jose, CA, USA, 2015.

[21] J. Shalev, "Loss aversion equilibrium," International Journal of Game Theory, vol. 29, no. 2, pp. 269–287, 2000.

[22] C. Hauert and G. Szabó, "Game theory and physics," American Journal of Physics, vol. 73, no. 5, pp. 405–414, 2005.

[23] F. C. Santos and J. M. Pacheco, "Scale-free networks provide a unifying framework for the emergence of cooperation," Physical Review Letters, vol. 95, no. 9, Article ID 098104, 2005.