electronics

MDPI

Article

Analyzing Miners' Dynamic Equilibrium in Blockchain Networks under DDoS Attacks

Xiao Liu [1], Zhao Huang [1,*], Quan Wang [1], Xiaohong Jiang [2], Yin Chen [3] and Bo Wan [1]

[1] School of Computer Science and Technology, Xidian University, Xi'an 710071, China; cantona@stu.xidian.edu.cn (X.L.); qwang@xidian.edu.cn (Q.W.); wanbo@xidian.edu.cn (B.W.)
[2] School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan; jiang@fun.ac.jp
[3] Graduate School of Media and Governance, Reitaku University, Kashiwa 277-8686, Japan; ychen@reitaku-u.ac.jp
* Correspondence: z_huang@xidian.edu.cn; Tel.: +86-187-9261-0378

Abstract: Proof of work (PoW) is one of the most widely used consensus algorithms in blockchain networks. It mainly uses the competition between mining nodes to obtain block rewards. However, this competition for computational power will allow malicious nodes to obtain illegal profits, bringing potential security threats to blockchain systems. A distributed denial of service (DDoS) attack is a major threat to the PoW algorithm. It utilizes multiple nodes in the blockchain network to attack honest miners to obtain illegal rewards. To solve this problem, academia has proposed a DDoS attack detection mechanism based on reinforcement learning methods and static game modeling methods based on mining pools. However, these methods cannot effectively make miners choose the strategy with the best profit over time when facing DDoS attacks. Therefore, this paper proposes a dynamic evolutionary game model for miners facing DDoS attacks under blockchain networks to solve the above problems for the first time. We address the model by replicating the dynamic equation to obtain a stable solution. According to the theorem of the Lyapunov method, we also obtain the only stable strategy for miners facing DDoS attacks. The experimental results show that compared with the static method, the dynamic method can affect game playing and game evolution over time. Moreover, miners' strategy to face DDoS attacks gradually shifts from honest mining to launching DDoS attacks against each other as the blockchain network improves.

Keywords: blockchain; DDoS attacks; electronic transaction; network layer; PoW; security threat

Citation: Liu, X.; Huang, Z.; Wang, Q.; Jiang, X.; Chen, Y.; Wan, B. Analyzing Miners' Dynamic Equilibrium in Blockchain Networks under DDoS Attacks. *Electronics* **2023**, *12*, 3903. https://doi.org/10.3390/electronics12183903

Academic Editor: Mehdi Sookhak

Received: 26 August 2023
Revised: 11 September 2023
Accepted: 13 September 2023
Published: 15 September 2023

1. Introduction

The PoW consensus algorithm is a widely used consensus algorithm for blockchain systems. PoW algorithm makes the blockchain nodes participating in the consensus through the network calculate a large number of unpredictable mathematical puzzles to prove the efforts of the nodes to obtain the right to get out of the block and the corresponding rewards. The process of competing with each other in terms of computing power to calculate the puzzle is called mining. The nodes in the blockchain network that participate in the mining process are called miners. The reward given to the miner that mines a new block is referred to as getting out of the block or mining reward [1]. Bitcoin is one of the most widely used blockchain systems that use PoW algorithms to maintain data consensus and ensure security [2]. The PoW algorithm can ensure the security of the Bitcoin system ledger and the impossibility of tampering with transactions [3]. However, many nodes (miners) must continuously compete to solve the puzzle to obtain the block reward. This competition, known as mining, consumes much computing power among miners and mining pools. Excessive competition and mining blocks can cause insecurity problems for miners. At the network layer, if malicious nodes forge IP addresses or send excessive numbers of network connection requests, the honest miners will lose their mining rewards. The malicious nodes

will obtain an illegal block reward by launching several types of attacks, such as denial of service (DoS) attacks, blockchain DoS (BDoS) attacks, and distributed DoS (DDoS) attacks on blockchain networks [4]. The occurrence of such problems brings huge mining reward losses and security threats to blockchain networks [5]. Among them, DDoS attacks are the most important security threat [6].

A DDoS attack is when multiple attackers in different locations launch simultaneous attacks on one or more targets over a network [7]. In DDoS attacks, the attacker cuts off the connection between the target node and the network through the network, resulting in no external network requests and traffic access. This brings huge economic losses to the target node [8]. However, DDoS attacks also frequently occur on blockchain networks [9]. DDoS attacks on blockchain networks mainly refer to malicious mining nodes controlling multiple nodes through the network to attack other honest mining nodes to obtain illegal mining rewards [9]. In the PoW algorithm based on the mining process, malicious miners usually initiate excessive network requests to honest miners [7,10]. Therefore, it is necessary to implement effective models and algorithms in the blockchain network environment based on the PoW algorithm to resist or reduce the loss caused by malicious miners launching DDoS attacks. Academics have proposed many methods to solve the DDoS attack problem in the blockchain network layer. At present, these methods can be mainly divided into the following categories: DDoS defense methods combined with blockchain technology, DDoS combination attacks combined with other blockchain attacks, and static game strategies based on the blockchain mining pool [10–17]. Among these existing studies, the use of a static game approach to mitigate DDoS attacks is the most effective [18–21]. The Nash equilibrium solution is a static game strategy. It means that after the game, any player who unilaterally changes their strategy under this strategy combination (the other players' strategies remain unchanged) will not improve their own payoff. In other words, the Nash equilibrium state is an optimal state in which the static game method prevents all players from playing an additional game [22]. Therefore, the research of these static methods is mainly to obtain the Nash equilibrium state with the optimal profit of the mining pool. These static game modeling methods can utilize a finite number of games and implement the Nash equilibrium optimal profit strategy value of the mining pool when the mining pool faces different DDoS attacks under the blockchain network. Thus, they can alleviate the loss caused by DDoS attacks on the mining pools to a certain extent [23,24]. However, there are some drawbacks and problems with these static game approaches. First, the way of modeling and solving the stable strategy of these static methods cannot reflect the dynamic evolution of the strategies of both sides of the game over time. Second, these methods cannot effectively reflect the changing trend of miners' game strategy selection of mining strategy probability with time and parameter changes when miners respond to DDoS attacks under different network environment parameters. Third, there is a lack of effective game theory methods in the current research to model DDoS attacks miners face. Therefore, it is necessary to establish a dynamic game model to implement the dynamic selection of the miners and its optimal profit mining strategy when facing DDoS attacks in blockchain networks.

To solve the above problems, this paper proposes an evolutionary game approach to mitigate the DDoS attack for the miners. We use the evolutionary game method to build a model of two miners with the same computing power facing DDoS attacks. We then find the stable solution by replicating the dynamic equation. The Ode45 function is a function to solve differential equations in Matlab, which can be used to solve the equilibrium solution of dynamic differential equations in evolutionary game models [17]. In different network environments [25], we use the ode45 function of Matlab libraries to solve the stable strategy solution of the replicated dynamic equation. The experimental results show that the model designed by us can better reflect the evolution trend over time and the changing trend of game probabilities when miners face DDoS attacks in dynamic games than in static games. In particular, the main contributions of this paper are as follows.

- To the best of our knowledge, this paper is the first to use a dynamic method to study the selection of the profitable optimal strategy for miners under DDoS attacks.
- We construct the miners' profits tables and dynamic replication equation based on a DDoS attack.
- We obtain the optimal strategy in different cases by analyzing various attack situations on the dynamic replication equation.
- By comparing static and dynamic games, the experimental results show that dynamic games have the advantages of allowing multiple games and a better game evolution when miners face attacks. To be clear, the better the network environment is, the more the miners will choose to launch an attack to obtain the best profit when facing DDoS attacks.

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 presents our design of a DDoS attack game theory module and solutions for miners in blockchain systems. The analysis of the system performance is in Section 4. Conclusions and future work are provided in Section 5.

2. Related Work

2.1. DDoS Attacks in Blockchain Systems

In blockchain systems, many consensus algorithms use mining as an essential tool to generate blocks. The consensus layer of the blockchain system controls miners when they compete with each other to generate blocks based on mining [26]. PoW, proof of stake (DPoS), proof of activity (PoA), and other standard blockchain algorithms are the most common consensus algorithms in the consensus layer, ensuring the security and data consistency of the blockchain system. The PoW algorithm is the most widely used consensus algorithm for blockchain systems, which uses multiple nodes' arithmetic power to mine for block rewards in the blockchain systems. As the most basic mining unit, miners face many security threats when competing for mining. A malicious node obtains a miner's block reward by malicious means. Block withholding attacks, selfish mining attacks, and Sybil attacks are ways to withhold attacks by malicious nodes to use a higher mining computing power or forge IP addresses to attack honest miners to obtain illegal profits [27]. These attacks bring significant security threats and losses to the blockchain system. Therefore, we must protect miners in case of aggression.

A DDoS attack is one of the most common attacks encountered at the network layer of a blockchain system. A DDoS attack is usually caused by malicious nodes launching excessive network requests to disconnect the network of honest miners and obtain illegal block rewards. Honest miners suffer significant losses when attacked by malicious nodes. The occurrence of this DDoS attack scenario poses a security threat and financial loss to honest miners [28]. Therefore, the main target of DDoS attacks against blockchain systems is to illegally obtain mining income and block rewards from mining pools and miners. There are few kinds of research on miners against DDoS attacks. The current study is mainly embodied in DDoS defense methods and new DDoS attacks in two aspects.

2.2. The DDoS-Based Combination Attacks in Blockchain Systems

Combination attacks based on DDoS attacks mainly refer to malicious nodes launching DDoS attacks in combination with methods such as incentives, creating redundant blockchain forks (selfish mining), and other methods to obtain higher mining revenues than a single DDoS attack. Currently, academics have researched and made some progress on the aspects of new combinatorial attacks based on DDoS attacks. Hayat et al. [11] proposed a multilayer combination attack method (ML-DDoS) based on DDoS attacks and smart contracts, which was designed to obtain more rewards from attackers. Wang et al. [12] designed a new mining attack, a selfish mining-based denial-of-service (SDoS) attack, which targeted the blockchain system based on the PoW mechanism and analyzed the gains and strategies of the attacker and the honest miners through game theory. Mirkin et al. [13] implemented a novel DDoS attack based on blockchain incentives called blockchain denial of service

(BDoS). The attacks utilized the blockchain's reward mechanism to induce rational miners to stop mining, thus bringing the PoW-based cryptocurrency system to a standstill. The attack did not require control over a large portion of the mining capacity, nor did it require constant resource consumption, making it more effective and dangerous than traditional DDoS attacks. Yaish et al. [29] proposed a combination of DDoS attacks by combining the characteristics of blockchain and Ethereum. This combination attack consumed the victim's resources and reduced its benefits by executing context and verifying inconsistencies.

2.3. Defense and Mitigation Methods for DDoS Attacks

There are more current approaches to DDoS defense and mitigation strategies in blockchain systems. These methods are mainly categorized into two main categories: detection of DDoS attacks and mitigation of DDoS attacks. The first category mainly detects the presence of DDoS attacks by detecting the presence of excessive network requests or abnormal traffic in the blockchain system. The second type of research mainly uses static game theory methods to model and solve the Nash equilibrium's optimal profit strategy solution for the two mining pools facing DDoS attacks [30].

At present, the anti-DDoS attack methods in the blockchain system are mainly to detect and defend against DDoS attacks by detecting excessive network requests and abnormal traffic. Ilyas et al. [31] introduced an efficient technique using optimization-based deep learning by considering the blockchain network and a smart contract for the detection and prevention of DDoS attacks. The traffic was analyzed based on the user request, and a verification using a smart contract in the blockchain system was made to find the authenticated user. The network responses were provided for the authenticated user, and the suspicious traffic was utilized for the detection of DDoS attacks using the poaching raptor optimization-based deep neural network. Yakubu et al. [32] used blockchain-based smart contracts and single-server queuing systems to achieve secure authentication of communication between devices in smart homes and protocols to resist DDoS attacks. This method could detect whether blockchain devices launched DDoS attacks in IoT environments by verifying that abnormal traffic existed during authentication. Houda et al. [33] proposed a new framework based on blockchain technology. The framework protected the privacy of blockchain networks and mitigated the hazards of security threats such as DDoS attacks and DoS attacks. Jmal et al. [34] proposed an ANN DDoS attack detection model based on an artificial intelligence approach to identify malicious traffic and optimize the traffic load as a way to identify the presence of DDoS attacks on blockchain networks.

The research on DDoS game modeling in the academic community mainly focuses on the static modeling and solving of the mining pool revenue. These research studies use static modeling methods such as zero-determinant games or repeated games to study the benefits of mining pools facing DDoS attacks [35–37]. Wu et al. [18] expressed the interactive competition of mining revenue between mining pools under the blockchain network in the face of DDoS attacks as a general and random game model and proposed an efficient Nash learning algorithm to obtain a near-optimal DDoS attack strategy that maximized the expected long-term utility. Johnson et al. [19] first proposed a model and optimal strategy approach for static games when mining pools faced DDoS attacks in a blockchain system environment. This model effectively alleviated the mining losses caused by DDoS attacks on two mining pools with different computing power. Guo et al. [38] proposed a blockchain-based distributed collective entrance defense (DCED) framework in which network traffic characteristics could be recorded and aggregated at the entrances of the satellite Internet (SI). Their method used static game theory to model blockchain nodes and could effectively resist DDoS attacks. Wang et al. [39] proposed static game-based strategies for mining activity analysis to mitigate DDoS attacks in blockchain networks. By solving the Nash equilibrium point of the static game, the transaction fee dilemma of the mining pool and the transaction fee strategy of the end user was realized. Sood et al. [40] proposed a profit mitigation model for DDoS attacks in mining pools based on the stochastic game method. The model took the cost of launching DDoS attacks by mining pools into

account in the modeling, which effectively mitigated the impact of changes in the network on the reduction in revenue that mining pools faced from DDoS attacks.

There has been some research on blockchain systems facing BWH attacks and selfish mining attacks in blockchain systems using dynamic games to solve the problem of decreasing their mining revenue. Huang et al. [5] proposed a dynamic evolutionary game model to mitigate the loss of revenue from BWH attacks faced by mining pools in blockchain systems. This dynamic game model was able to obtain the optimal solution for mining pools facing BWH attacks with different penalties and rewards. Kesavan et al. [41] presented a dynamic evolutionary game method of attacking the proof-of-work consensus based on selfish mining attacks. Their model used an evolutionary game for the first time to study the mining losses caused by selfish mining attacks to alleviate the reduction in mining pool revenue. Mighan et al. [42] used a dynamic evolutionary game model to model the probability of using the Ethernet data distribution network. The model allowed for the accurate modeling of data propagation and forks in blockchain systems. The authors also effectively addressed the issue of BWH attacks being able to degrade the performance of the Ethernet network using the dynamic game approach modeling.

2.4. Challenges in Current Research

The existing work on blockchain DDoS attacks can address the problems encountered to a certain extent. These types of approaches only boost the revenue of the mining pool that launched the attack. However, these efforts face more new issues and challenges. The DDoS-based combination attack methods can reduce attack costs while effectively enabling malicious mining pools to obtain higher mining revenues. However, these combination attack methods cannot alleviate, detect, and protect the losses of honest node mining benefits caused by combination attacks. These methods also cannot mitigate the revenue loss from DDoS attacks on mining pools that mine honestly and cannot effectively detect the presence of DDoS attacks in advance. To solve this problem, many research methods have been proposed to corrupt the DDoS attacks in blockchain networks. These methods can effectively use artificial intelligence to detect excessive network requests and abnormal traffic to prevent DDoS attacks. However, these methods only consider detecting the existence of DDoS attacks in advance and thus defending against them in advance. However, these methods do not consider the problem of revenue loss from honest mining when miners or mining pools face DDoS attacks during the mining process. In order to solve these problems, academics have gradually proposed static game models to mitigate the mining losses caused by DDoS attacks. The static game method is somewhat effective in mitigating the loss of mining revenue from mining pools. However, there are a number of problems and challenges associated with them. Static game modeling can only use a limited number of games. This approach is unable to perform multiple games dynamically and effectively reflect the convergence trend of parameter changes for different probabilities of honest mining pools or miners under different DDoS attack scenarios of game changes. Based on the research of BWH attack and selfish mining attack evolutionary game model, it can be proved that the dynamic evolutionary game method can effectively solve the problem of mitigating the reduction in revenue of mining pools or miners in the mining process when the blockchain system faces attacks. The success of the research work on these other attacks also suggests that dynamic games can similarly be used for the blockchain system's DDoS attack gain mitigation problem. However, current research work on DDoS attacks lacks effective dynamic modeling. This is the key issue that needs to be addressed in this paper.

Due to the above problems, we need to propose a new method to solve the problem that miners cannot effectively obtain the best benefits when facing DDoS attacks. In particular, we propose a dynamic evolutionary game model to establish the benefits of miners facing DDoS attacks under the blockchain network and find the optimal mining strategy according to different network environment conditions. The dynamic game model that we designed contains three main parts: model description, model building, and optimal strategy solving.

In the following part of this paper, we specifically describe the design and solution process of the model.

3. The Proposed Evolutionary Game Theory Model and Solutions

3.1. Problem Description and Hypothesis

In this section, we assume a scenario where two miners with the same computational power face a decrease in revenue from DDoS attacks. We analyze the problems faced by this scenario and model the revenue problems faced by this scenario through parameters. In this paper, we consider the scenario where two miners with the same arithmetic power under the same mining pool face a DDoS attack. A typical scenario of a miner launching a DDoS attack in a blockchain network is shown in Figure 1. From Figure 1, we can see multiple mining pools competing for mining rewards through the network. Multiple mining pools perform honest mining to obtain the block rewards. However, they do not launch DDoS attacks to attack other mining pools over the network. Here, we assume pool 1 mines a block and receives a block reward from the pool manager, while the other pools do not receive the mining rewards. Mining pool 1 receives a mining reward value of R. Two miners of the same arithmetic power are mining under the same pool 1. When miner A and miner B both mine honestly in pool 1 at the same time, their share of the mining revenue is half of the revenue of pool 1, and the value is R. When miner A launches a DDoS attack on miner B, miner A cannot continue to mine honestly in the mining pool due to insufficient computing power. Mining pool 1 has only miner B mining honestly. At this time, the mining computing power of miners in mining pool 1 is half of the honest mining of miners, so the total mining revenue obtained by the miners is $\frac{R}{2}$. Therefore, miners A and B mine below pool 1 with an average return of $\frac{R}{4}$. However, the miner A does not want to spend arithmetic power to mine rewards honestly. Therefore, miner A consumes part of its arithmetic power to launch DDoS attacks on miner B through the network to gain illegal mining revenue. As shown in Figure 1, miner A launches DDoS attacks on miner B and receives a mining reward. Miner B loses wd's mining reward. w represents the network environment impact factor. d represents the illegal mining reward caused by miner A launching DDoS attacks when the network condition is very good (in the ideal network state, the value of w is 1). The pool manager penalizes the attacking pool and rewards the honest pool based on whether the miner attacks or not. The amount of reward and punishment is set to a. Finally, miner A launches an attack to gain mining revenue but is also punished by the pool manager for the attack. Miner B is rewarded for mining honestly but also suffers mining losses due to the attacks. The specific parameter description and four attack scenarios are elaborated and analyzed in the following contents.

We refer to this scenario and extend it to other DDoS attack scenarios for miners to make the following assumptions and analyze the whole problem. In this paper, Table 1 is established to explain the parameters and the corresponding description of the parameters. Through the relevant parameters in Table 1, we can conduct a rational analysis, and model, and find the solution to different situations facing DDoS attacks under the same mining pool. To simplify the establishment of the game model, this paper only considers the scenario of two miners with the same computing power in the same mining pool. The description of this problem and the assumptions are as follows.

(1) This paper assumes that all miners only mine in one mining pool and are not allowed to switch to other mining pools at will.

(2) We assume that the computing power of the entire mining pool is constant. The total block production reward obtained from the mining pool is assumed to be R. The mining pool only has two miners, A and B, with the same computing power. When miners A and B are both honest miners, the average payoff is $\frac{R}{2}$. When one of the miners launches a DDoS attack, the average honest mining gain for A and B is $\frac{R}{4}$. When A and B launch DDoS attacks on each other, miners A and B both earn 0 for honest mining.

(3) When a particular miner launches a DDoS attack, the loss of the honest miner is wd. The quality of the network environment is represented by the network coefficient w,

which is $0 \leq w \leq 1$. d is the damage caused by malicious miners to honest miners when the network is in an ideal state. Then, the network situation can cause malicious miners to launch DDoS attacks to incur damage. This paper assumes that the better the network condition, the higher the loss to honest miners. Thus, wd represents the illegal rewards obtained by the miner which launches a DDoS attack.

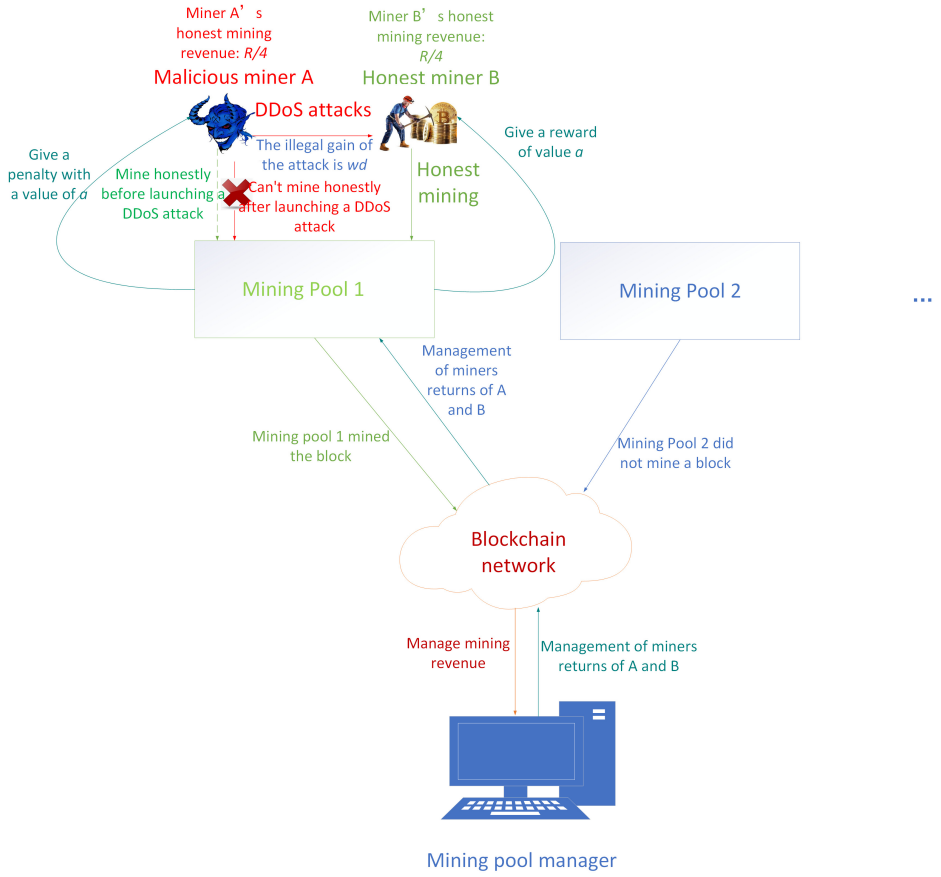

Figure 1. A scenario in which miners of a blockchain system face a DDoS attack.

Table 1. DDoS attack modeling parameters for miners.

Parameters	Description and Function of Parameters
R	The total profit allocated by the pool manager when a single mining pool mines in the blockchain system.
d	The illegal revenue gained by the attacker or the revenue lost by the attacked miner.
a	(1) When miners mine honestly with the same mining pool, the pool manager gives the reward to honest miners. (2) When a malicious miner launches a DDoS attack, the attacker is punished by the mining pool manager.
w	Network environment coefficient.
f_1	The miner returns from honest mining.
f_2	The miner returns when launching DDoS attacks.
$\overline{f}$	Average returns for miners facing DDoS attacks.
$F(x)$	The dynamic equation of replication for x and time t.
$F'(x)$	The first derivative of $F(x)$ with respect to the probability x of honest mining.
x	The probability that the miners mine honestly.
$x_i(i = 1, 2, 3 \ldots)$	Solve the replicated dynamic equations to obtain the optimal policy values of multiple candidates that a miner may choose under the attack return model of this paper.
x^*	Deterministic mining strategies under different degrees of network environment.

(4) Because miners are mining in the same pool, the pool manager punishes miners with a penalty of a when they launch a DDoS attack. Similarly, when there is a DDoS attack in the same mining pool, the mining pool manager gives a reward of a to the honest miners.

(5) To simplify the establishment and solution of the model, this paper needs to meet the following restrictions. This paper does not consider the cost of DDoS attacks by miners. We also do not allow miners who mine in one pool to casually switch to mining in a different pool.

3.2. Design and Implementation of DDoS Attacks' Evolutionary Game Model for Miners

In this section, we need to build our evolutionary game model according to the above problem analysis. Our assumptions and analysis of DDoS attacks are similar to those in the literature [18,24,33]. We need to set up separate tables of block reward payoffs for miners A and B. Then, miners in the same mining pool will choose two strategies when facing attacks: launching a DDoS attack (D) and honest mining (H). According to whether miner A and miner B launch DDoS attacks or not, attacks can be divided into the following four scenarios: (H, H), (H, D), (D, H), and (D, D).

(1) First, we consider the (H, H) case. This attack scenario is shown in Figure 2 below. The revenue that the entire pool receives from mining blocks is R. Miners A and B have the same computing power and mine under the mining pool. Therefore, the pool receives revenue R and splits it equally between miners A and B. Then, in this case, miners A and B both receive a block-producing reward of $\frac{R}{2}$.

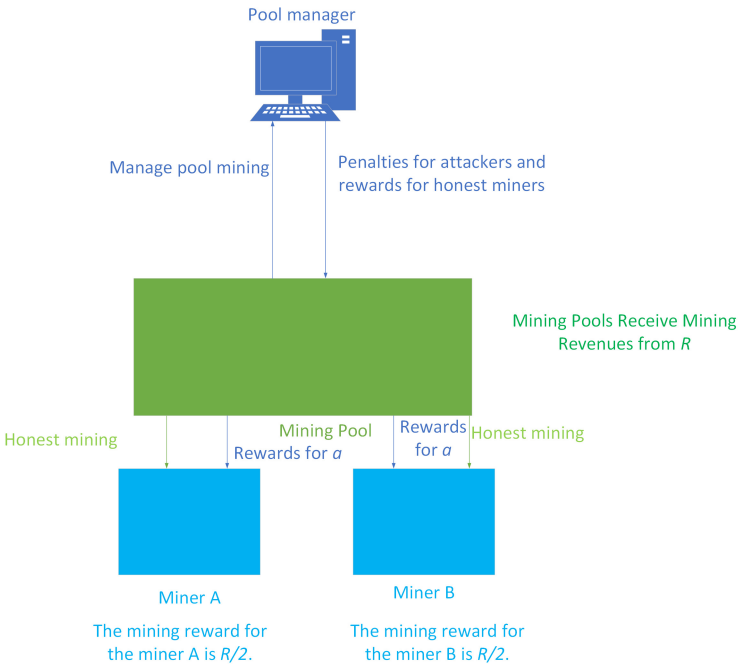

Figure 2. A scenario in which both miners mine honestly.

(2) Next, we consider the case of (H, D). This means that miner B launches a DDoS attack on miner A while miner A is mining honestly. In this case, only miner A mines honestly in the mining pool, and miner B can only sustain DDoS attacks on miner A due to insufficient computing power and cannot continue to mine honestly. At this point, there is only one miner A in the mining pool whose computing power is normal and honest. Therefore, the mining power of the miner, in this case, is half of the original mining power of both miner A and miner B. The total revenue from honest mining of the entire pool is R. Both miners earn an average payoff of $\frac{R}{2}$ by mining honestly. While the pool's honest mining power is cut in half in this case, the total mining profit to miners A and B is also cut in half by $\frac{R}{2}$. Therefore, each miner can only reap $\frac{R}{4}$ because the mining power is reduced

by half. Miner B launches a DDoS attack on miner A to obtain a mining reward of wd. Miner A suffers from a DDoS attack from B that loses wd's block reward. The pool manager rewards A with a for honest mining. Thus, miner A's payoff in this situation is $\frac{R}{4} + a - wd$. Miner B receives $\frac{R}{4}$ for honest mining. B launches a DDoS attack, and the mining pool manager penalizes it a. Miner B launches a DDoS attack and receives a block reward of wd from miner A. Thus, miner B's payoff in this situation is $\frac{R}{4} - a + wd$. The specific attack situation is shown in Figure 3 below.

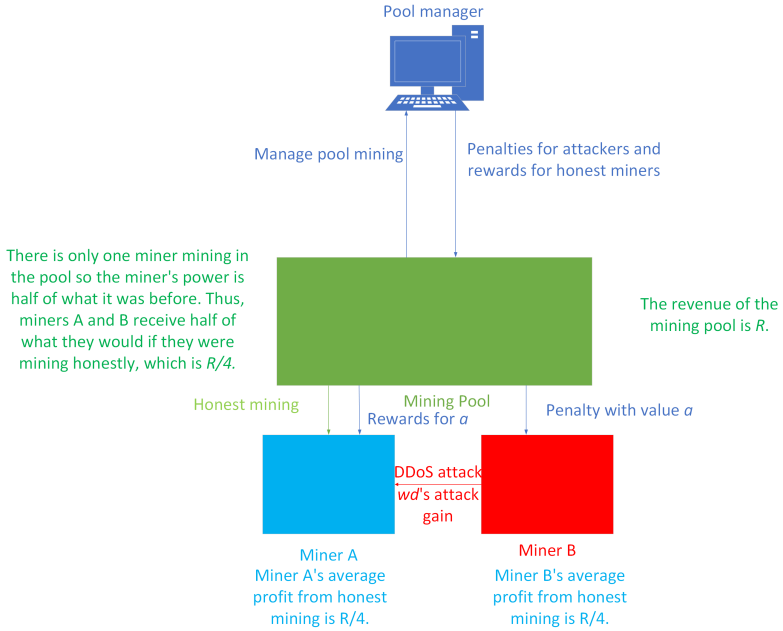

Figure 3. Miner B launches a DDoS attack on miner A, while A mines honestly.

(3) Then, we consider the case of (D, H). This means that miner A launches a DDoS attack on miner B while miner B is mining honestly. The miners in the pool currently have half the computational power of case 1. Miners A and B receive an average of R for honest mining. Similar to the case (H, D), except in this case, A is the attacker, and B is the victim. Similarly to case 2, A 's payoff in this case is $\frac{R}{4} - a + wd$. B 's payoff in this case is $\frac{R}{4} + a - wd$. The attack is shown in Figure 4 below.

(4) Finally, we consider the (D, D) case. In this case, miners A and B launch DDoS attacks and cannot mine honestly. Thus, the average return of A and B for honest mining in the pool is 0. Miner A suffers a DDoS attack from B and loses wd's block reward. However, A launches a DDoS attack and receives a block reward of wd from miner B. Since A launches a DDoS attack, the mining pool manager penalizes miner A with an amount equal to a. Thus, the reward of miner A in this case is $-a$. Since A and B both attack and A and B have the same amount of power, miner B and A have the same payoff in this situation. Thus, in this case, miner B 's payoff is also $-a$. This attack situation is shown in Figure 5 below.

After the above model is established, we can establish the profit and income tables of miner A and B, respectively, according to the profits under the four attack situations. In the game model of a DDoS attack, the income table of miner A is shown in Table 2 below.

Table 2. The revenue of miner A when attacked by DDoS attacks.

Pool A \ Pool B	Honest Mining (H)	DDoS Attacks (D)
Honest mining (H)	$\frac{R}{2}$	$\frac{R}{4} + a - wd$
DDoS attacks (D)	$\frac{R}{4} - a + wd$	$-a$

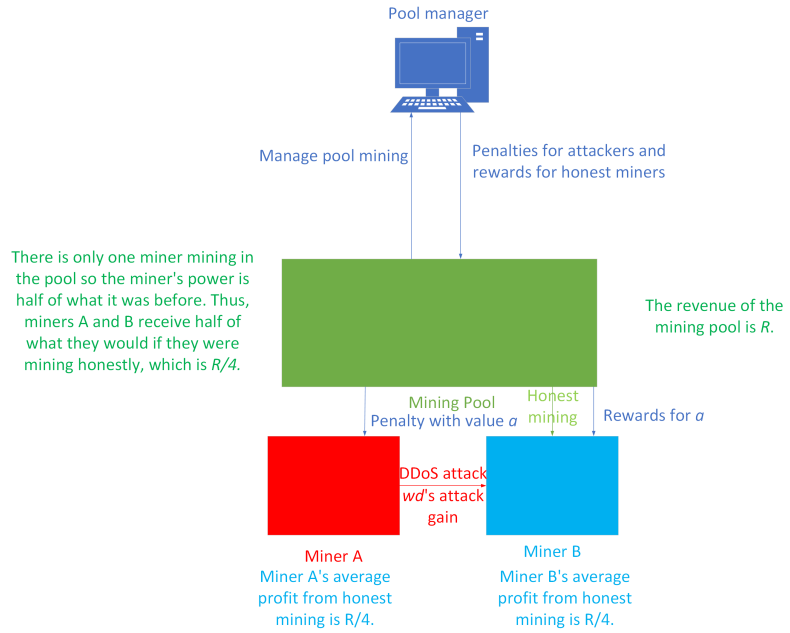

Figure 4. Miner A launches a DDoS attack on miner B, while B mines honestly.

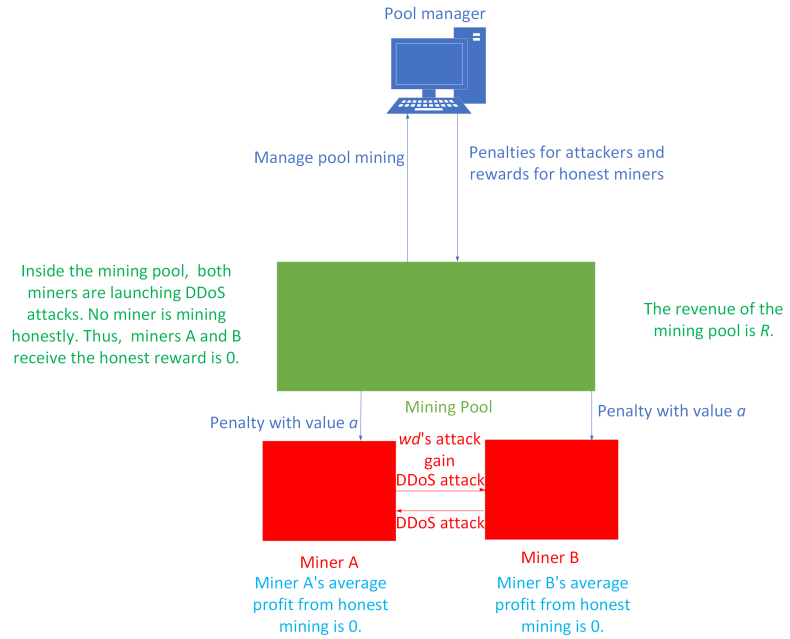

Figure 5. Miner A and miner B launch DDoS attacks on each other.

Each element in the table represents miner A's payoff when miner A and miner B perform honest mining (H) or launch a DDoS attack (D). Similarly, the income table of miner B is described in Table 3 below.

Table 3. The revenue of miner B when attacked by DDoS attacks.

Pool B \ Pool A	Honest Mining (H)	DDoS Attacks (D)
Honest mining (H)	$\frac{R}{2}$	$\frac{R}{4} - a + wd$
DDoS attacks (D)	$\frac{R}{4} + a - wd$	$-a$

After establishing the model and the income table of miners A and B, we need to develop a stable solution by setting the average income of miners to establish a dynamic

replication equation [39]. We assume miners A and B mine honestly with probability x. The likelihood of an attack being selected is $1-x$. x is $0 \leqslant x \leqslant 1$. We use x^* as the stable solution to the dynamic equation. Then, this paper establishes the complementary strategies to obtain the optimal benefits through the values of each steady state. Through Tables 2 and 3, we can obtain the average earnings of honest mining by miners. We assume that a miner's average payoff of honest mining is f_1. The definition of f_1 is shown in Equation (1) below .

$$f_1 = x * \frac{R}{2} + (1-x) * (\frac{R}{4} + a - wd). \tag{1}$$

Similarly, we can use f_2 to represent the profit that a dishonest miner launches DDoS attacks, which is described in Equation (2).

$$f_2 = x * (\frac{R}{4} - a + wd) + (1-x) * (-a). \tag{2}$$

Therefore, from Equations (1) and (2), we can conclude that the average expected return of the miner is $\overline{f}$ in Equation (3).

$$\begin{aligned} \overline{f} &= x * f_1 + (1-x) * f_2. \\ &= x * [x * \frac{R}{2} + (1-x) * (\frac{R}{4} + a - wd)] + (1-x) * [x * (\frac{R}{4} - a + wd) + (1-x) * (-a)] \\ &= x^2 * \frac{R}{2} + x(1-x) * \frac{R}{2} + (1-x)^2 * (-a) \end{aligned} \tag{3}$$

From the above equation, we can conclude that the replication equation under this model is $F(x)$. $F(x)$ represents the steady state of honest mining probability x over time. Then, the dynamic replication equation $F(x)$ implemented in this paper is listed as follows in Equation (4).

$$\begin{aligned} F(x) &= dx(t)/dt \\ &= x(f_1 - \overline{f}) \\ &= x[f_1 - x * f_1 - (1-x) * f_2] \\ &= x(1-x)(f_1 - f_2) \\ &= x(1-x)[x * \frac{R}{2} + (1-x) * (\frac{R}{4} + a - wd) - x * (\frac{R}{4} - a + wd) - (1-x) * (-a)] \\ &= x(1-x)(\frac{R}{4} - wd + 2a - ax) \end{aligned} \tag{4}$$

We set the value of the dynamic replication equation $F(x)$ to 0, and we can obtain three steady-state deals of the evolutionary game, which is listed in the following Equation (5).

$$x_1 = 0, x_2 = 1, x_3 = \frac{R - 4wd + 8a}{4a} \tag{5}$$

We derive three possible stable states for this DDoS attack model by solving the dynamic replication equation. The three solutions of the dynamic replication equation, which are represented by $x_i (i = 1, 2, 3 \ldots)$, are described in Equation (5). x_i denotes the multiple optimal policy values computed by the replication dynamic equation. When x_i is composed of uncertain values x_3, such as the network environment parameter w, the value range of $x_i = x_3$ is $x_3 \in R$. R is the whole set of real numbers. Next, we need to discuss the range of values of x_3 by comparing x_3 with the extreme values of probability 0 and 1. According to the method of solving the evolutionary game solution in reference [43], we divide it into three cases and discuss the stable state x^* in each case.

Through these three steady-state values, this paper can select the network coefficient w according to the situation of each steady-state solution. We also use the solution method of the evolutionary game to analyze which strategy benefits the miners best under each stable solution.

3.3. Steady-State Solutions

Through the three steady-state values, we can obtain the optimal mining strategy for different network environments w. By solving the problem of miners facing DDoS attacks and selecting the optimal mining strategy, we can also obtain the value range of the network environment coefficient w. Since the reward value a which is given by the pool manager must be positive, the case $a < 0$ is not considered in this paper. In the ideal state of the network case, the profit d of malicious miners launching DDoS attacks is also a fixed value. The range of d is $d \geq 0$. The first derivative of $F(x)$ with respect to x is $F'(x)$. We need to find out the unique mining strategy solution x^* under different network conditions through the change in network condition coefficient w. The value of x^* is chosen between the steady-state values x_1, x_2, and x_3. The $x_i (i = 1, 2, 3 \ldots)$ value satisfying $F'(x) < 0$ is the stable strategy solution x^* in each case of different network situations w when facing the DDoS attacks. However, among the three steady states obtained by the replication dynamic equation, $x_1 = 0, x_2 = 1$ are fixed values, and only the value of x_3 is uncertain. Therefore, we need to determine the value range of the network environment coefficient w by distinguishing the values of x_1, x_2, and x_3. At the same time, we also need to determine which steady-state solution makes $F'(x) < 0$ in x_1, x_2, and x_3 according to the range of values of x_3. This solution is the optimal mining strategy for miners with different x_3 values and the range of the network environment w. That is to say, we need to obtain the slope image of $F'(x)$ by discussing the value of x_3 in different cases to obtain the stable strategy [44].

Case A: $x_3 \leq 0$ means that $\frac{R-4wd+8a}{4a} \leq 0$, $d \geq 0$, and $a > 0$.

The reward and penalty a given to miners by the mining pool manager is a fixed value. The profit from successful pool mining is also a fixed value of R. DDoS attacks are launched at a fixed rate of d in the best network environments. The only parameter value that changes in steady state x_3 is the network environment coefficient w. The choice of miner strategy depends on the efficiency of network communication. The greater the value of w, the higher the damage inflicted by malicious miners on honest miners. In this case, simply setting $x_3 \leq 0$ takes the value range $\frac{R-4wd+8a}{4a} \leq 0$. The probability of honest mining can still be $x_1 = 0$ and $x_2 = 1$. From $\frac{R-4wd+8a}{4a} \leq 0$, we can conclude that the range of the network coefficient w is $\frac{R+8a}{4d} \leq w \leq 1$. The phase diagram of the replication dynamic is shown in Figure 6 below. We can analyze the optimal solution for DDoS attacks faced by miners in a relatively good network environment through Figure 6. The steady-state value is determined by replicating the dynamic equation with a negative slope at the intersection of the abscissa [44]. In this case, the equilibrium strategy solution satisfying $F'(x) < 0$ is $x^* = x_1 = 0$. Therefore, in case A, the best mining strategy for miners facing DDoS attacks is $x^* = x_1 = 0$. Therefore, in a good network environment, the optimal strategy for miners is to launch DDoS attacks against each other to obtain the optimal revenue.

$x^* = 0$ means that in a good network environment, miners choose to attack each other for the best profit over time. The main reason is that the network is excellent, malicious miners can launch DDoS attacks through the network and obtain more illegal block production rewards than when the network is in a harsh environment. The better the network environment, the more miners tend to choose to launch DDoS attacks to gain more revenue. Therefore, all miners will choose the best profit by launching DDoS attacks against each other.

Case B: $x_3 \geq 1$ means that $\frac{R-4wd+8a}{4a} \geq 1$, $d \geq 0$, and $a > 0$.

In this case, we can conclude by $\frac{R-4wd+8a}{4a} \geq 1$ that the value range of w is $0 \leq w \leq \frac{4a+R}{4d}$. This means that w is very small, and the network environment is poor. The phase diagram of the replication dynamic is shown in Figure 7 below. We can analyze it by replicating the phase diagram of the dynamic equation that the steady state, in this case, is $x^* = 1$. In case B, the equilibrium strategy solution satisfying $F'(x) < 0$ is $x^* = x_2 = 1$. Therefore, in a harsh network environment, miners will eventually choose the honest mining strategy to gain the best mining rewards.

The reason for the occurrence of case B is that miners receive fewer mining rewards by launching DDoS attacks when the network condition is harsh. If the miners profit less, they will choose the safe mining strategy with increasing games to gain the best profit. At the same time, when the network is not good, miners which do not know each other's mining status will not easily launch attacks. Therefore, all miners will eventually choose the honest mining strategy as the best way to profit over time.

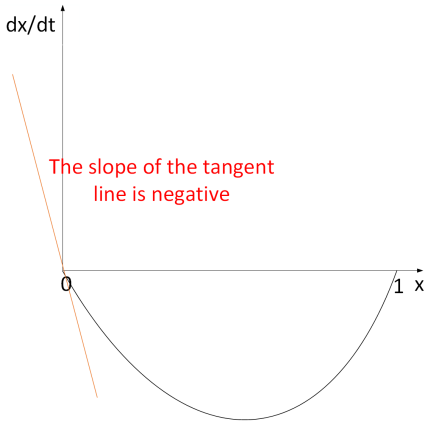

Figure 6. Replication dynamic phase diagram of attack case A.

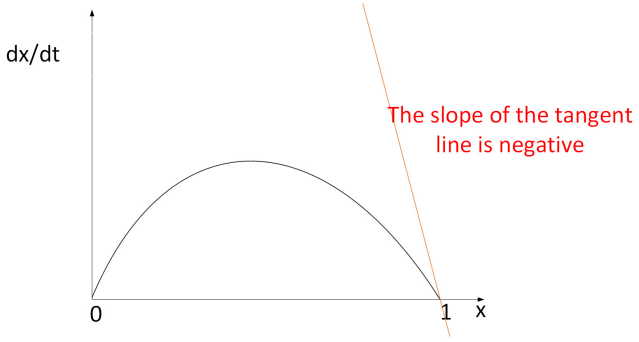

Figure 7. Replication dynamic phase diagram of attack case B.

Case C: $0 < x_3 < 1$ means that $0 < \frac{R-4wd+8a}{4a} < 1$, $d > 0$, and $a > 0$.

$0 < \frac{R-4wd+8a}{4a} < 1$ means that the network coefficient w ranges in $0 \leq \frac{4a+R}{4d} < w < \frac{8a+R}{4d} \leq 1$. This means the network is in a medium condition, The phase diagram of the replication dynamic is shown in Figure 8 below. From Figure 8, we can see that the optimal mining strategy, in this case, is $x_3 = \frac{R-4wd+8a}{4a}$. In case C, the equilibrium strategy solution satisfying $F'(x) < 0$ is $x^* = x_3 = \frac{R-4wd+8a}{4a}$. In a medium environment network, miners will choose the best profit from honest mining with a probability of x_3.

The reason for this is that because the network is under medium conditions, the miners will obtain almost the same payoff from launching a DDoS attack or from honest mining. All miners with different initial probabilities of honest mining will not choose the extreme option of honest mining or attack. Miners will eventually select the mixed strategy with the likelihood of honest mining with the best profit over time. Therefore, miners choose the mixed strategy in the medium network environment with an honest mining probability of x_3 to gain the best profit.

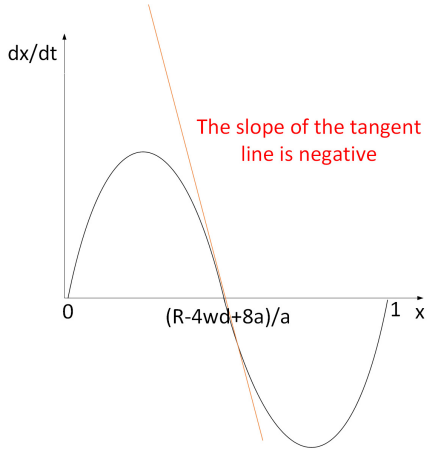

Figure 8. Replication dynamic phase diagram of attack case C.

Based on the above Section 3.3, we summarized the optimal strategy x^* for various network situations in Table 4. Table 4 describes the specific parameter ranges and optimal policy solutions in each network case. Table 4 lays a good foundation for the parameter setting and experimental analysis of dynamic and static game experiments in Section 4.

Table 4. Evolutionary stability strategy of miners facing DDoS attacks.

Network Environment Coefficient w	Evolutionary Steady-State Strategy x^*	Analysis
$\frac{R+8a}{4d} \leq w \leq 1$	$x^* = 0$	A good network environment corresponds to Case A
$0 \leq w \leq \frac{4a+R}{4d}$	$x^* = 1$	A harsh network environment corresponds to Case B
$0 \leq \frac{4a+R}{4d} < w < \frac{8a+R}{4d} \leq 1$	$x^* = \frac{R-4wd+8a}{4a}$	A medium network environment corresponds to Case C

4. Experiment and Results

The experimental simulation in this paper was divided into two main parts: a static game experiment and an evolutionary game experiment. In this section, our experiments' main goal was to validate the steady state of the evolutionary dynamic game model solution. We also implemented three static game experiments on the model to realize the Nash equilibrium point problem of miners facing DDoS attacks under static game conditions. The detailed description and performance analysis of the experiments is as follows. First, we selected the appropriate parameters and built the game experiment form according to the designed DDoS attack miner model. Second, we used the set model parameters to establish a static game model to solve the Nash equilibrium solution. Third, we conducted three static game experiments to achieve our designed model's optimal Nash equilibrium solution. We used Matlab R2022b to conduct evolutionary game modeling for miners in the same mining pool facing a DDoS attack in the blockchain system. Finally, we compared the design model in the static Nash equilibrium and the dynamic evolutionary game and analyzed the experimental results. The experimental results confirmed the correctness and effectiveness of the dynamic game model we designed.

We divided each part of the dynamic and static game experiment into three small experiments according to the strength coefficient w of the network. We also set the initial value parameters as $a = 6, d = 45, R = 60$. The actual game situations are shown in the following three experiments. We set the values of w to 0.1, 0.5, and 0.8, respectively, according to different network conditions. By comparing six experiments on static games and dynamic evolutionary games, this paper implemented the optimal selection strategy of miners under DDoS attacks in different network environments.

The settings of the six experimental parameter values and the solutions obtained are described in Table 5 below.

Our three settings of comparative static and dynamic evolutionary games experiments were assigned and solved according to Table 5. By changing the value of w to create separate network environments, we divided the whole experiment into three parts in both static game and dynamic evolutionary game. We set the corresponding parameters to observe the game state of miners facing DDoS attacks under different network environments. At the same time, we obtained the final miner's stable state x^* in each case under three other experimental conditions. Comparative experiments showed that the model designed by us had more game iterations in dynamic games than in static games and could show the trend of game evolution and convergence. The experimental results also showed that the experimental x^* was consistent with the theoretical value obtained by evolutionary game modeling and solving. The three experiments and analyses are described below.

Table 5. Comparison table of specific parameters and values corresponding to the static and dynamic game experiments.

One Miner Honest Mining Profit in One Same Mining Pool R	Illegal Profits of Miners Launching DDoS Attacks d	Degree of Punishment or Reward by the Pool Manager a	Network Environment Coefficient w	Evolutionary Steady-State Strategy x^*	Analysis
$R = 60$	$d = 45$	$a = 6$	$w = 0.1$	$x^* = x_2 = 1$	Nash equilibrium point for Experiment Section 4.1.1 of the static game and the solution obtained in experiment Section 4.2.1 correspond to case A in Section 3.3
$R = 60$	$d = 45$	$a = 6$	$w = 0.5$	$x^* = x_3 = \frac{R-4wd+8a}{4a} = \frac{60+0.5*45*4-8*6}{4*6} = 0.75$	Nash equilibrium point for Experiment Section 4.1.2 of the static game and the solution obtained in experiment Section 4.2.2 correspond to case C in Section 3.3
$R = 60$	$d = 45$	$a = 6$	$w = 0.8$	$x^* = x_1 = 0$	Nash equilibrium point for Experiment Section 4.1.3 of the static game and the solution obtained in experiment Section 4.2.3 correspond to case B in Section 3.3

4.1. Static Game Experiment

We mainly carried out three experiments in this section to realize the Nash equilibrium state of the static game of the designed model when miners face DDoS attacks according to references [45,46]. The purpose of the static game experiment was to serve as a contrast experiment for the following dynamic evolutionary game experiment. The main idea of the comparison experiment was to reflect the advantages of miners in realizing the dynamic evolutionary game when facing DDoS attacks by comparing our designed model in the case of static and dynamic games. As can be seen from Table 4 above, our static game experiment was divided into three subexperiments according to the different network environments w. The implementation and analysis of the three subexperiments are shown below.

4.1.1. Analysis of Game Strategy under the Bad Network Environment

After completing the experimental parameterization, we implemented the experiment on the optimal gain of miners facing DDoS attacks under the environment with bad network conditions in this section. The static optimal solution of DDoS attacks faced by miners in a bad network environment is realized by solving the Nash equilibrium. In the first subexperiment, we set the network environment coefficient to $w = 0.1$. According to Table 4 above, we set the global parameters as an honest miner mining gain to $R = 160$, the illegal gain for miners launching DDoS attacks to $d = 45$, and the penalty and reward for the mining pool manager to $a = 6$. The results of Experiment 1 are shown in Figures 9 and 10 below. We obtained the static Nash equilibrium solution of the designed model in the case of a bad network environment.

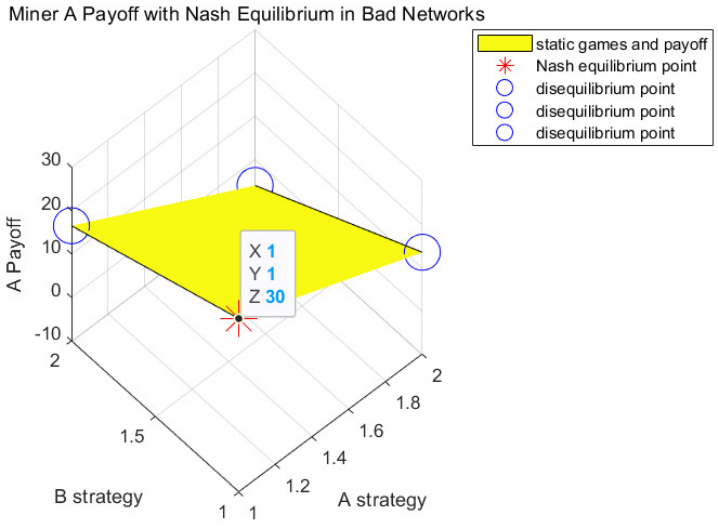

Figure 9. In a bad network environment, miner A faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

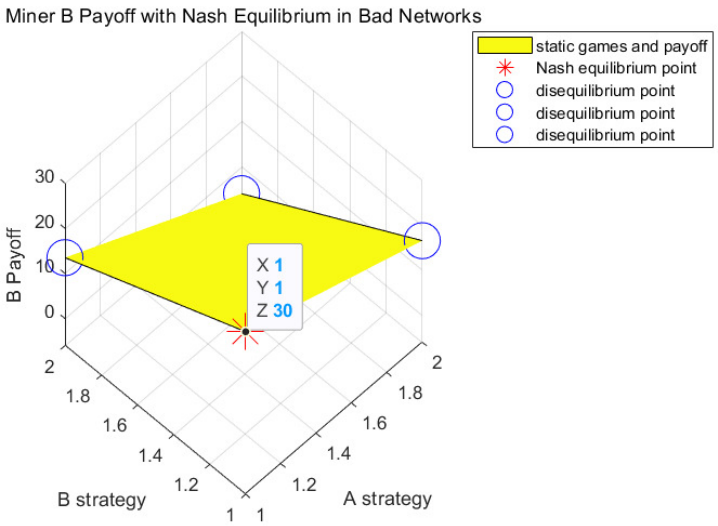

Figure 10. In a bad network environment, miner B faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

In the following Figures 9 and 10, the red coordinates represent the Nash equilibrium optimal solution, and the blue coordinates represent the nonequilibrium points. A value equal to one on the X-axis in Figure 9 indicates that miner A chooses the honest mining strategy, and a value equal to zero indicates that mining pool A chooses to launch a DDoS attack. Similarly, a value of one on the Y-axis means that miner B chooses the honest mining

strategy, and a value of zero on the Y-axis means that miner B chooses to launch a DDoS attack. The Z-axis represents the miner's optimal return when the Nash equilibrium is reached. As can be seen from Figure 9, the Nash equilibrium value of miners A and B is $(1, 1)$ when the network condition is not good. These results indicate that in the static game case, miners A and B choose honest mining for optimal profit when facing DDoS attacks. The optimal profit obtained by miner A is 30. Similarly, Figure 10 shows that miner B chooses honest mining for the best gain in the static game situation. Miner B's final optimal payoff is also 30.

4.1.2. Analysis of Game Strategy under the Medium Network Environment

When network conditions are harsh conditions, miners choose to mine honestly for optimal returns. As the network situation gradually improves, the changing scenarios occurring in the DDoS attack gains faced by miners will be reflected in the results of the medium static experiments. In this experiment, we set the value of the network environment parameter to $w = 0.5$. According to Table 4 above, we set the global parameters as an honest miner mining gain to $R = 160$, the illegal gain for miners launching DDoS attacks to $d = 45$, and the penalty and reward for the mining pool manager to $a = 6$. The static game experiment results of miner A and miner B are shown in Figures 11 and 12, respectively. In Figures 11 and 12, the coordinates marked in blue are nonequilibrium points, and the coordinates marked in red are Nash equilibrium points.

As can be seen from Figure 11, the Nash equilibrium points obtained by miner A in the static game when facing DDoS attacks in the revenue model designed in this paper are $(1, 2, -1.5)$ and $(2, 1, 31.5)$, respectively. This means that in the medium network environment, miner A faces DDoS attacks, and the optimal solution obtained using the static game approach to achieve the Nash equilibrium is a mixed strategy. The $(1, 2, -1.5)$ strategy means that miner A chooses to mine honestly, but miner B decides to launch a DDoS attack to achieve a static Nash equilibrium. Miner A's best payoff is -1.5. The $(2, 1, 31.5)$ strategy means that miner B chooses to mine honestly, but miner A chooses to launch a DDoS attack to achieve a static Nash equilibrium. Miner A's best payoff is 31.5.

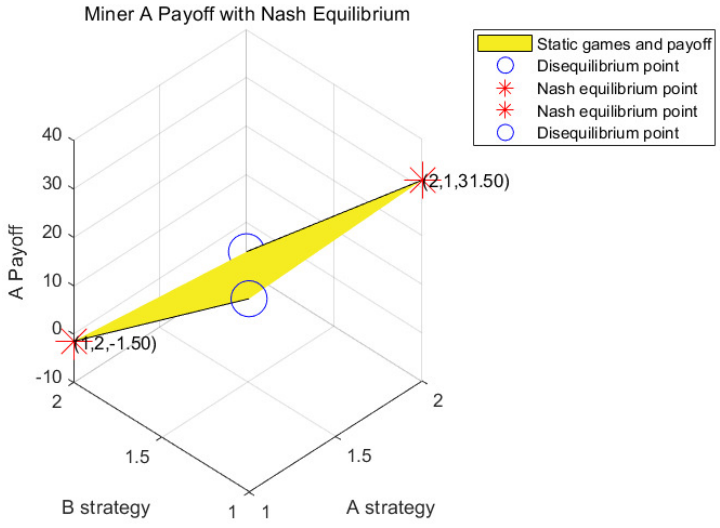

Figure 11. In a medium network environment, miner A faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

As can be seen from Figure 12, the Nash equilibrium points obtained by miner B in the static game when facing DDoS attacks in the revenue model designed in this paper are $(1, 2, 31.5)$ and $(2, 1, -1.5)$, respectively. $(1, 2, 31.5)$ means that miner B chooses the optimal profit from launching DDoS attacks when reaching Nash equilibrium, and miner A chooses the optimal profit from honest mining. The optimal equilibrium return for both A and B is 31.5. $(2, 1, -1.5)$ means that miner B chooses to launch honest mining when the Nash

equilibrium is reached, and miner A chooses to launch DDoS attacks to make the best profit. The optimal equilibrium payoff for both A and B is -1.5.

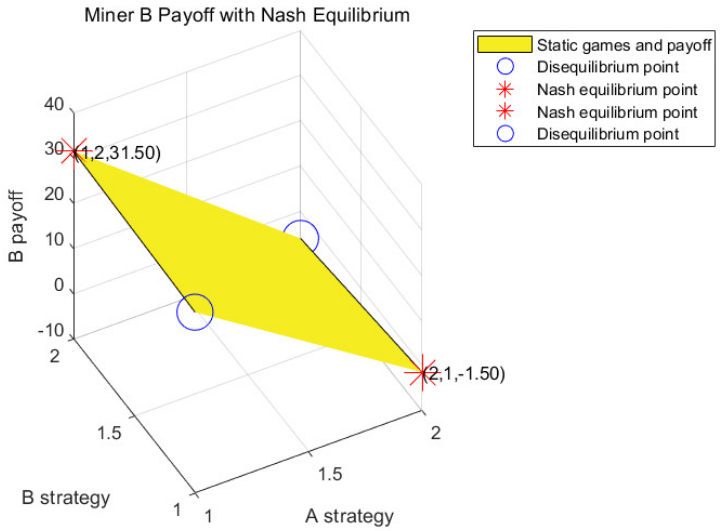

Figure 12. In a medium network environment, miner B faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

4.1.3. Analysis of Game Strategy under the Good Network Environment

In medium network environments, miners facing DDoS attacks choose multiple mining strategies to coexist for optimal profits. How the network situation can be further improved in the medium case and how it can affect the miners' strategy changes is what needs to be achieved in this section of the static game experiments. The experimental results of the Nash equilibrium point performance of miners A and B facing DDoS attack to achieve a static game are shown in Figures 13 and 14 below. In this experiment, we set the value of the network environment parameter $w = 0.8$. According to Table 4 above, we set the global parameters as an honest miner's mining gain to $R = 160$, the illegal gain for miners launching DDoS attacks to $d = 45$, and the penalty and reward for the mining pool manager to $a = 6$. The specific experimental results are shown in Figures 13 and 14 below. We can see from Figures 13 and 14 that the coordinates marked in blue are nonequilibrium points, and the coordinates marked in red are Nash equilibrium points.

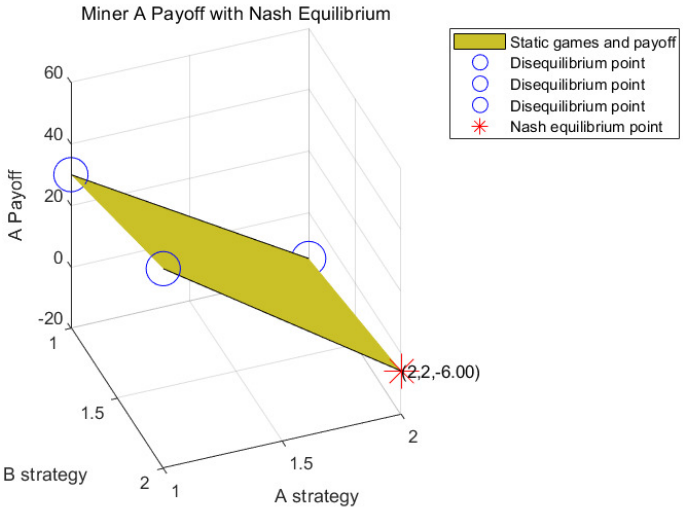

Figure 13. In a good network environment, miner A faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

According to Figure 13 below, the Nash equilibrium point of miner A's static game when facing a DDoS attack is $(2, 2, -6)$. The strategy of $(2, 2, -6)$ means that in the case of good network conditions, miner A and miner B choose to launch DDoS attacks to obtain the best profit. Miner A's optimal payoff in the static Nash equilibrium is -6. Similarly, it can be seen from Figure 14 that the Nash equilibrium point of miner B is also $(2, 2, -6)$. Miner B also makes the best profit by launching DDoS attacks when the network is good. Miner B's best Nash equilibrium payoff is the same as miner A's, that is, -6.

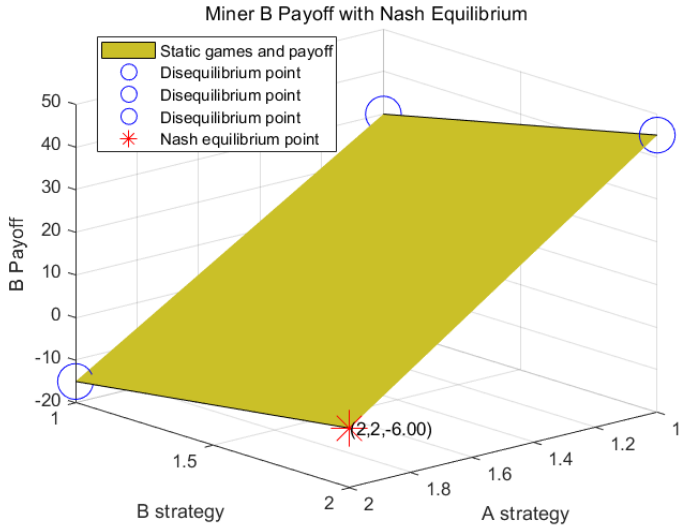

Figure 14. In a good network environment, miner B faces the strategy of obtaining the best reward in a static game scenario by DDoS attacks.

4.2. Evolutionary Game Experiment

4.2.1. Analysis of Game Strategy under a Harsh Network Environment

After completing the static game experiment, we needed to realize the advantages of the dynamic game by comparing the results of the dynamic game experiment with the static game experiment. We implement the analysis of the optimal strategy for the change in revenue of the dynamic game for miners facing DDoS attacks based on the harsh network environment in this section. We also compare the results with static game experiments in Section 4.1.1. In this case, we modeled the earnings of miners through Matlab. In the case of a bad network environment, we conducted an evolutionary game experiment for the miners facing a DDoS attack under the blockchain system. In that experiment, we set the network coefficient to $w = 0.1$. The experimental miner evolutionary game with a pool network environment is shown in Figure 15. From Figure 15 below, we can derive the strategy choice when the miners mining in the same pool face a DDoS attack under the condition of a poor network. We set the miners' initial honest mining probabilities from 0.1 to 0.9. Through the experiment, we observed and analyzed which strategies miners with different possibilities chose to make the best profit after being attacked.

Figure 15 presents the evolution trend of the miner strategy facing a DDoS attack in the same pool. From Figure 15, we can see that the horizontal coordinate represents the time t, and the vertical coordinate represents the initial probability x of honest mining in the mining pool. The curves of different colors in Figure 15 represent pools with different initial values for honest mining with different probabilities x. Initially, we set the miners to mine honestly with a probability from 0.1 to 0.9. The mining probability of honest miners with different probabilities changes over time, and after multiple game iterations, all probabilities eventually tend to one. Thus, the optimal strategy value of the iteration is one, and the convergence time of the game is about 0.35 s. This means that the final reward of the game is that all the miners will choose honest mining to gain the best profits. In the case of bad network conditions, the final strategy selected by the miners in the face of a DDoS attack has a probability of one to mine honestly in the last game time. The

experiment corresponds to case B in Section 3.3 above, in which the result $x^* = x_2 = 1$ is consistent with the experiment.

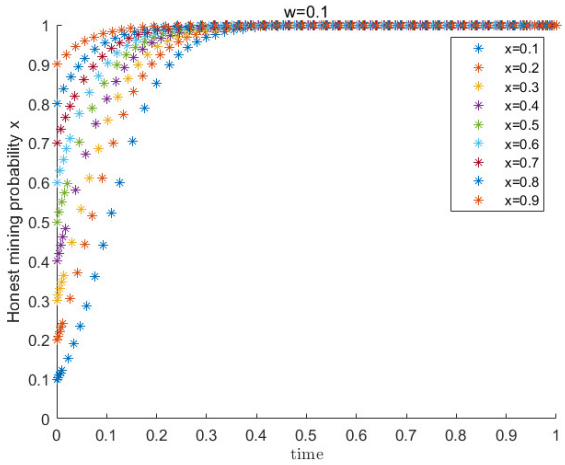

Figure 15. In a poor network environment, the miners face the strategy of obtaining the best reward with time t using DDoS attacks ($w = 0.1, x^* = 1$).

The reasons why miners face DDoS attacks in harsh network environments are as follows. First, due to the poor network environment, miners do not understand the network environment situation and dare not venture to launch DDoS attacks. Due to the unstable network environment, all miners choose honest mining strategies. Second, the illegal gains wd obtained by miners launching DDoS attacks in this experiment are proportional to the network environment coefficient w. The value of the network coefficient w becomes low if the network environment is bad. Miners which have to launch DDoS attacks in hostile network environments to gain illegal mining revenue wd will also have a smaller network coefficient value. This diminishing return on attacks can lead to miners launching attacks for far less illicit gain than they would bring in from their own peaceful and honest mining. In the end, all miners prefer the honest mining strategy that obtains more revenue rather than launching a DDoS attack.

Compared with the results of static game experiment Section 4.1.1 above, the results of our designed model in the dynamic evolutionary game experiment are the same as those of the static game. Both miner A and miner B choose the honest mining strategy to make the best profit under the harsh network conditions. However, the static game can only reflect that the honest mining strategy is the optimal strategy for miners in the harsh network environment through one game. There are some problems and defects in static game experiments under a bad network environment. First, the static game can only be played once in a bad network environment. The limit of the number of games can not effectively reflect the correctness of the optimal strategy when miners face DDoS attacks. Second, the static game can only obtain the optimal strategy by solving the Nash equilibrium solution. This method cannot reflect the game trend of the miner game with different probabilities of mining towards the optimal strategy over time through multiple game iterations. We realized the optimal strategy in multiple game environments by the method of game iteration in the harsh environment dynamic game experiments. At the same time, we set different initial mining probabilities by different colored curves. Through multiple game iterations in the dynamic experiments, we obtained the tendency of miners with different mining probabilities to converge to the optimal strategy over time.

4.2.2. Analysis of Game Strategy under a Medium Network Environment

When the network conditions are bad, miners change over time and choose honest mining strategies. Then, in this section, by increasing the value of the network environment coefficient w, we analyzed the trend of the change in the dynamic returns of miners. The

purpose of this experiment was to verify whether the strategy selected by miners in the face of DDoS attacks in the medium network was consistent with the optimal strategy obtained in case C in Section 3.3 of the dynamic evolutionary game model analysis. In the case of the medium network environment, we conducted an evolutionary game experiment for the miners facing DDoS attacks under the blockchain system. In that case, we set the network coefficient to $w = 0.5$. The experimental miner evolutionary game with a medium network environment is shown in Figure 16. From Figure 16 below, we can derive the strategy choice when the miners mining in the same pool face a DDoS attack. We set the miners' initial honest mining probabilities from 0.1 to 0.9. Through this experiment, we observed and analyzed which strategies miners with different possibilities chose to make the best profit after being attacked.

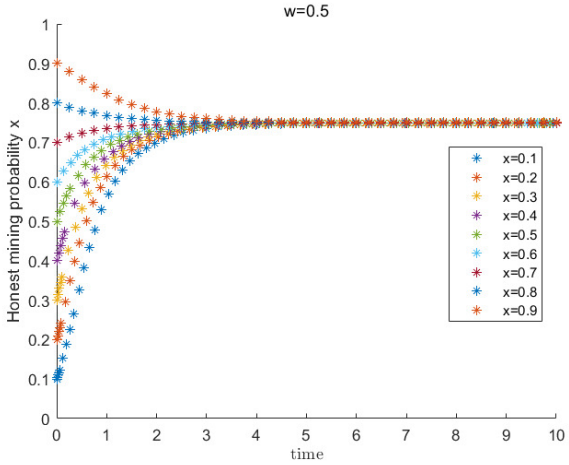

Figure 16. In a medium network environment, the miners face the strategy of obtaining the best reward with time t using DDoS attacks ($w = 0.5, x^* = 0.75$).

From Figure 16, we can see that in a medium network environment, all the miners with different probabilities will eventually choose to mine honestly with a certain probability and make the best profit. The probability of honest mining x^* depends on the values of a, d, R, w. We still set the initial miner's honest mining probability x from 0.1 to 0.9 on the Y-axis. The tendency of the initial values of these different probabilities to change over time in the game is represented by different colored curves on the Y-axis. We find that all miners finally approach honest mining with a probability of 0.75 in about 4 s. This means that the network miner chooses the mixed strategy of honest mining with a probability of 0.75 in the medium environment to gain the best profit. This means that the stable strategy chosen by the miner, in this case, is $x^* = x_3 = 0.75$. The experimental results are consistent with case C in Section 3.3 above, proving our experiment's correctness and validity.

The reasons why miners facing DDoS attacks choose a hybrid strategy of honesty and launching DDoS attacks in a medium network environment are as follows. First, some miners think that the network environment is good enough to launch attacks for better returns as the network situation improves. As a result, some of the miners decide to launch DDoS attack strategies. Other miners still believe that the current moderate network conditions are not enough to make them change their original honest mining strategy, so this group of miners does not easily change their strategy to stick to honest mining. Second, the value of the illegal revenue obtained by miners launching DDoS attacks increases as the network environment improves. This motivates some miners to abandon the strategy of mining honestly in the pool for revenue and willingly accept punishment from the pool manager for launching DDoS attacks for illegal revenue. This can lead to a situation where some miners decide to mine honestly while others decide to launch DDoS attacks.

Compared with the results of static game experiment Section 4.1.2 above, the results of our designed model in the dynamic evolutionary game are the same as those of the static

game. In the medium network, miners A and B have two Nash equilibrium game points $(1, 2)$ and $(2, 1)$ in the static game experiment. This means that miners facing DDoS attacks in the static game scenario have a certain probability of making the best profit by launching a DDoS attack or a certain probability of making the best profit by honest mining. In the case of a medium network, the miners choose to use a mixed mining strategy. That means that the miners decide to mine honestly or launch DDoS attacks to obtain the best rewards. The Nash equilibrium solution of the static game strategy is consistent with the optimal strategy of the dynamic game in the medium network condition. However, the inability to effectively quantify the probability of a mixed strategy occurring is the most significant drawback of static games in medium network environments. In a medium-scale network environment, we cannot analyze through static game experiments the exact probability of the optimal miner strategy of honest mining and the probability of launching a DDoS attack. However, this problem was solved by a numerical simulation in our dynamic game experiments. We achieved this by setting the initial values to miners with different probabilities of honest mining. The probability values ranged from 0.1 to 0.9. We found that all miners mining with different probabilities eventually chose the strategy with honest probability $x = 0.75$ for optimal mining returns after many iterations of the game through a dynamic evolutionary game. This addresses the inability of static game experiments to quantify mixed-strategy probabilities in a moderate network environment. This solves the problem where static game experiments cannot effectively reflect the convergence trend and change in the game when miners face DDoS attacks.

4.2.3. Analysis of Game Strategy under a Good Network Environment

Mining pools in moderate network environments gradually shift towards launching DDoS attack strategies. Then, the dynamic trend of the optimal mining strategy for miners facing DDoS attacks under better network conditions than the medium environment is illustrated in the experiments in this section. In this case, we set $w = 0.8$ and the probability of miners to initially mine honestly x from 0.1 to 0.9. The experimental miner evolutionary game with a better network environment is shown in Figure 17. From Figure 17 below, we can see that the curves with different colors represent the game trend of honest miners with different probabilities over time. The game iteration changes over time with different colors for the initial probability of mining, but all the curves eventually tend to zero. Therefore, the value of x^*, in this case, is $x^* = x_1 = 0$. This means that in such a situation, miners would choose to launch DDoS attacks against each other to make the best profit.

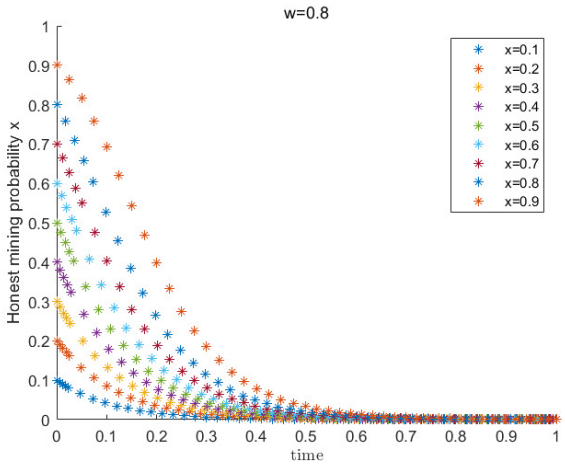

Figure 17. In a good network environment, the miners face the strategy of obtaining the best reward with time t using DDoS attacks ($w = 0.8, x^* = 0$).

From Figure 17, we can see that in the case of a good network environment, all the probabilities of miners mining with different honest mining probabilities eventually tend

to $x = 0$ at about $t = 0.6$ s. The experimental results illustrate that miners facing DDoS attacks choose to launch DDoS attacks against each other to obtain optimal mining rewards when the network state w is relatively good. The experimental results are in agreement with the dynamic game stabilizing solution case B, which was obtained by the dynamic game analysis in Section 3.3 above. The optimal solution obtained from the experimental results and the optimal solution found in case B of Section 3.3 above are both $x^* = 0$, which shows the correctness of our experimental results and the validity of the model.

In a better network environment, miners choose to launch DDoS attacks against each other to gain optimal profits for the following reasons. First, the network environment becomes better than a medium network, and more miners abandon the strategy of spending arithmetic power to mine honestly in the pool for revenue. Miners assume that the network environment is better and that all other miners use the network to launch DDoS attacks themselves in order to maximize illegal profits. As time goes on and multiple iterations of the game are played, all of the miners choose to make the optimal profit by attacking each other's strategies. Second, the network conditions become better and the value of the gain wd for a miner launching a DDoS attack increases more than it does in the case of the medium network. Miners that initially followed an honest mining strategy in moderate network environments also gradually adopt the more profitable strategy of launching DDoS attacks through multiple iterations of the game. Eventually, miners in medium network environments choose a mixed strategy that gradually shifts to launching DDoS attacks to profit optimally due to changes in the network environment.

Compared with the results of static game experiment Section 4.1.3 above, the results of our designed model in the dynamic evolutionary game are the same as those of the static game. In a relatively good network environment, miners choose to profit optimally by launching DDoS attacks against each other. This result is consistent with the dynamic game experiment results under good network conditions. The inability to effectively characterize how miners with different probabilities of honest mining converge to an optimal strategy over multiple game iterations is the main drawback of static game experiments in a well-networked environment. In order to solve this problem, we also set up different colored curves to represent the miners with different initial values of the mining probability through the numerical simulation experiments within the dynamic game experiments. We obtained the evolution curves of the change in miners towards the steady state $x^* = 0$ with different probabilities of honest mining through multiple game iterations and a time-varying evolution in our dynamic game experiments.

4.3. Analysis of Experimental Results

Therefore, the condition of the blockchain network affects the choice of the optimal profit-making strategy for miners facing DDoS attacks. Meanwhile, the dynamic game can reflect the advantage of the convergence trend of the miner's game over the static game experiments in solving the problem of the miner's gain from facing DDoS attacks. Specific experimental phenomena and results are detailed in the following according to the three cases of network conditions, and the dynamic and static game comparison results are divided into four aspects of analysis and elaboration.

(1) When the network in the pool is good, miners know how each other is doing. Since the network coefficient w is directly proportional to the illegal blocking reward obtained by launching DDoS attacks, miners gain more profits by launching DDoS attacks. In this case, all miners with different honest probabilities eventually choose to launch DDoS attacks to earn higher returns as time goes by and the number of games increases. Therefore, in a good network environment, all miners attack each other within 0.6 s.

(2) When the network is in a moderate condition, all miners do not go to the extreme of simply honestly mining or launching DDoS attacks. This is because miners with a low initial value of honest mining profit even if they launch DDoS attacks. Since the illegal income from DDoS attacks is not as good as the network environment, miners with a high probability of honest mining also lower the value of x and gain higher rewards. Therefore,

miners of all possibilities choose the mixed game strategy to obtain the optimal block-out reward.

(3) When the network in the pool is bad, all the miners need to know each other's status. Since the network coefficient w is directly proportional to the illegal blocking reward obtained by launching DDoS attacks and the network condition is deplorable, miners receive little benefit from launching DDoS attacks, and attacking the mining pool manager also brings a certain degree of punishment to miners. As a result, miners at this point do not gain as much from launching DDoS attacks as they do from honest mining. Therefore, miners with different probabilities of initial mining value eventually choose the game strategy of honest mining to obtain the most block reward in the lousy network environment.

(4) The experimental results of static games are consistent with those of dynamic evolutionary games, proving our model's validity. Through comparative experiments in three different network environments, we can see that the dynamic game method used in this paper has more games than the static game method and can show the trend of multiple games over time by miners with different probabilities of honest mining.

5. Discussion

Discussion point 1: What is the practical impact of the DDoS gain mitigation model designed in this paper on the blockchain industry?

Answer:

The first discussion point is mainly to explain the practical significance of our model. Currently, there are security threats and hidden dangers in the blockchain system. Attacks such as selfish mining attacks, block interception attacks, and DDoS attacks exist in blockchain systems to illegally obtain mining rewards from honest-mining miners [5]. Selfish mining attacks are used to illegally gain access to the benefits of the public chain by creating a private chain outside of the public chain. Block retention attack is to attack miners to withhold the mining rewards of honest miners to achieve the purpose of their own illegal gain. DDoS attacks are the security threats present in blockchain networks that we focused on in this paper. Our model is effective in making blockchain systems using PoW consensus algorithms effectively mitigate mining losses from DDoS attacks without the need to detect the number of network requests and abnormal traffic in advance. This can increase the security of blockchain systems that use the PoW consensus algorithm, such as Bitcoin. At the same time, this paper analyzed different network situations through the game theory approach to make miners choose the optimal mining strategy through multiple game iterations. This is a useful reference for miners using the Bitcoin system to choose appropriate mining strategies under different networks when they face DDoS attacks.

Discussion point 2: What are the shortcomings of the model designed in this paper?

Answer:

The second issue is mentioned in our future work section. It is mainly about what are the shortcomings of our current work and what can be improved. Our model has not yet taken into account the cost of launching a DDoS attack, the distribution of proceeds from DDoS attacks faced by multiple miners, and the fact that miners do not have the same mining arithmetic power.

First, this paper only considered the problem of two miners with the same arithmetic power facing a DDoS attack. In a real situation, blockchain system cluster nodes' arithmetic power is different. At the same time, the number of mining cluster nodes is much more than two. In the next step, we will extend the model designed in this paper to the scenario of multiple miners with different arithmetic power for an in-depth study, in order to meet the demand for security in real blockchain systems.

Second, in order to simplify the modeling, we do not consider the cost of launching DDoS attacks in this paper. This modeling approach does not meet the complex security situaton of miners in an actual blockchain network. In following work, we will take the

factors of attack cost and parameter representation of different values of punishment and reward into account to further improve the model designed in this paper.

6. Conclusions

In this paper, we proposed an evolutionary game model for miners facing DDoS attacks. The establishment and solution of this model can be effective enough to protect miners from DDoS attacks. We also obtained the optimal mining strategies of miners in different network environments by replicating the dynamic equation methods. We finally conducted comparative experiments between static and dynamic games for the designed model. The experimental results showed that miners facing DDoS attacks gradually shifted from an honest mining strategy to the profit optimization of launching DDoS attacks as the network conditions became better. The results of the dynamic and static comparison experiments showed that the dynamic game method had the advantage of being able to quantify the mixed strategies of miners facing DDoS attacks under medium network conditions and reflecting the trend of the change in the optimal strategy from multiple game iterations of mining pools with different probabilities. However, the static game approach could only represent the optimal strategies and returns of miners. The static game method could not realize the quantification of the probability of mixed strategies and the trend of game convergence dynamics. This suggests that the use of the dynamic game approach in this paper has advantages over the static game approach. The experimental results proved the effectiveness and correctness of the dynamic game model we designed.

7. Future Work

This paper effectively mitigates the revenue loss from DDoS attacks by modeling the dynamic game in the case of two mining pools with the same arithmetic power. However, there are many areas for improvement in the current work of this paper. First, the DDoS reward model's assumptions did not consider the cost of launching a DDoS attack by the miners. Second, the modeling assumed that the two pools had the same computational power. We did not consider the possibility of multiple mining pools with different computing power, which is not widely applicable. Therefore, we want to carry out the following in-depth research on this work in the future. Third, we modeled and solved the benefits of DDoS attacks faced by miners in a simulated environment. We did not conduct an actual experimental performance analysis of the model on a real blockchain system. In order to solve these problems, we need to carry out further in-depth research into the model of this paper to meet the requirements of real blockchain systems in future work. Future work will contain three main parts: research on asymmetric arithmetic miner game, research on the gain of multiminer game, and research on the security model of miner DDoS attacks under a real blockchain system. The specific work will be as follows:

(1) We will take the cost of launching DDoS attacks and the number of nodes launching attacks into consideration in a newly designed game model in the future so that the model establishment is more in line with the requirements of the existing blockchain system.

(2) We will add the case of multiple miners with different arithmetic power to the modeling and solving in this paper in future work. We will also provide an in-depth study of the problem of modeling multiple and solving the optimal gain of multiple miners and multiple mining pools facing DDoS attacks.

(3) In future work, we will improve the model designed in this paper so that it can be applied to real blockchain systems to meet the security requirements of real applications.

Author Contributions: Conceptualization, Q.W., X.J. and Z.H.; methodology, Z.H. and X.L.; software, Z.H. and X.L.; validation, Z.H., B.W., Y.C. and X.L.; writing—original draft preparation, X.L. and Z.H.; writing—review and editing, Z.H., Y.C., X.J. and Q.W.; supervision, X.J. and Q.W.; project administration, Z.H., Y.C., Q.W. and B.W.; funding acquisition, Q.W., B.W., X.J. and Z.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under grant 61972302, in part by the Fundamental Research Funds for the Central Universities under grant XJS220306, in part by the Natural Science Basic Research Program of Shaanxi under grant 2022JQ-680, in part by the Science and Technology Program of Guangzhou under grant SL2022A04J00404, in part by the Foundation of National Key Laboratory of Human Factors Engineering under grant 6142222210101, in part by the key industry innovation chain projects of Shaanxi, China under grant 2021ZDLGY07-04, and in part by the Key Laboratory of Smart Human Computer Interaction and Wearable Technology of Shaanxi Province.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would like to thank the Editors and Reviewers for their contributions to our manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Meneghetti, A.; Sala, M.; Taufer, D. A Survey on PoW-based Consensus. *AETiC* **2020**, *4*, 8–18. [CrossRef]
2. Lepore, C.; Ceria, M.; Visconti, A.; Rao, U.P.; Shah, K.A.; Zanolini, L. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Mathematics* **2020**, *8*, 1782. [CrossRef]
3. Xu, J.; Wang, C.; Jia, X. A Survey of Blockchain Consensus Protocols. *ACM Comput. Surv.* **2023**, *55*, 278. [CrossRef]
4. Yadav, A.K.; Singh, K.; Amin, A.H.; Almutairi, L.; Alsenani, T.R.; Ahmadian, A. A Comparative Study on Consensus Mechanism with Security Threats and Future Scopes: Blockchain. *Comput. Commun.* **2023**, *12*, 102–115. [CrossRef]
5. Liu, X.; Huang, Z.; Wang, Q.; Wan, B. An Evolutionary Game Theory-Based Method to Mitigate Block Withholding Attack in Blockchain System. *Electronics* **2023**, *12*, 2808. [CrossRef]
6. Huang, Z.; Wang, Q. A PUF-based Unified Identity Verification Framework for Secure IoT Hardware via Device Authentication. *World Wide Web* **2020**, *2*, 1057–1088. [CrossRef]
7. Kumari, P.; Jain, A.K. A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures. *Comput. Secur.* **2023**, *127*, 103096. [CrossRef]
8. Mittal, M.; Kumar, K.; Behal, S. Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Comput.* **2023**, *27*, 13039–13075. [CrossRef]
9. Waseem, M.; Adnan Khan, M.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. [CrossRef]
10. Guru, A.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2604. [CrossRef]
11. Hayat, R.F.; Aurangzeb, S.; Aleem, M.; Srivastava, G.; Lin, J.C.-W. ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments. *IEEE Trans. Eng. Manag.* **2022**, *2022*, 1–14. [CrossRef]
12. Wang, Q.; Xia, T.; Wang, D.; Ren, Y.; Miao, G.; Choo, K.-K.R. SDoS: Selfish Mining-Based Denial-of-Service Attack. *IEEE Trans. Inform. Forensic Secur.* **2022**, *17*, 3335–3349. [CrossRef]
13. Mirkin, M.; Ji, Y.; Pang, J.; Klages-Mundt, A.; Eyal, I.; Juels, A. BDoS: Blockchain Denial-of-Service. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020; pp. 601–619. [CrossRef]
14. Liu, J.; Wang, X.; Shen, S.; Yue, G.; Yu, S.; Li, M. A Bayesian Q -Learning Game for Dependable Task Offloading Against DDoS Attacks in Sensor Edge Cloud. *IEEE Internet Things J.* **2021**, *8*, 7546–7561. [CrossRef]
15. Baek, U.-J.; Ji, S.-H.; Park, J.T.; Lee, M.-S.; Park, J.-S.; Kim, M.-S. DDoS Attack Detection on Bitcoin Ecosystem Using Deep-Learning. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4. [CrossRef]
16. Jiang, S.; Yang, L.; Gao, X.; Zhou, Y.; Feng, T.; Song, Y.; Liu, K.; Cheng, G. BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks. *Secur. Commun. Netw.* **2022**, *2022*, 1608689. [CrossRef]
17. Zhang, Y.; Gai, K.; Zhu, L.; Qiu, M. An Auxiliary Classifier GAN-Based DDoS Defense Solution in Blockchain-Based Software Defined Industrial Network. In *Smart Computing and Communication*; Qiu, M., Lu, Z., Zhang, C., Eds.; Lecture Notes in Computer Science; Springer Nature: Cham, Switzerland, 2023; Volume 13828, pp. 319–328. [CrossRef]
18. Wu, S.; Chen, Y.; Li, M.; Luo, X.; Liu, Z.; Liu, L. Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools. *IEEE/ACM Trans. Netw.* **2020**, *28*, 874–887. [CrossRef]
19. Johnson, B.; Laszka, A.; Grossklags, J.; Vasek, M.; Moore, T. Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools. In *Financial Cryptography and Data Security*; Böhme, R., Brenner, M., Moore, T., Smith, M., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8438, pp. 72–86. [CrossRef]

20. Boreiri, Z.; Azad, A.N. A Novel Consensus Protocol in Blockchain Network Based on Proof of Activity Protocol and Game Theory. In Proceedings of the 2022 8th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2022; pp. 82–87. [CrossRef]
21. He, Q.; Wang, C.; Cui, G.; Li, B.; Zhou, R.; Zhou, Q.; Xiang, Y.; Jin, H.; Yang, Y. A Game-Theoretical Approach for Mitigating Edge DDoS Attack. *IEEE Trans. Depend. Secur. Comput.* **2022**, *19*, 2333–2348. [CrossRef]
22. Amini, H.; Bichuch, M.; Feinstein, Z. Decentralized payment clearing using blockchain and optimal bidding. *Eur. J. Oper. Res.* **2022**, *309*, 409–420. [CrossRef]
23. Khanum, S.; Mustafa, K. A Systematic Literature Review on Sensitive Data Protection in Blockchain Applications. *Concurr. Comput.* **2023**, *35*, e7422. [CrossRef]
24. Saad, M.; Njilla, L.; Kamhoua, C.; Kim, J.; Nyang, D.; Mohaisen, A. Mempool Optimization for Defending Against DDoS Attacks in PoW-Based Blockchain Systems. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; pp. 285–292. [CrossRef]
25. Tan, Y.; Huang, X.; Li, W. Does blockchain-based traceability system guarantee information authenticity? An evolutionary game approach. *Int. J. Prod. Econ.* **2023**, *264*, 108974. [CrossRef]
26. Bao, Q.; Li, B.; Hu, T.; Sun, X. A Survey of Blockchain Consensus Safety and Security: State-of-the-Art, Challenges, and Future Work. *J. Syst. Softw.* **2023**, *196*, 111555. [CrossRef]
27. Guo, H.; Yu, X. A Survey on Blockchain Technology and Its Security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
28. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain-Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors* **2022**, *22*, 1094. [CrossRef] [PubMed]
29. Yaish, A.; Qin, K.; Zhou, L.; Zohar, A.; Gervais, A. Speculative Denial-of-Service Attacks in Ethereum. *Cryptol. ePrint Arch.* **2023**, *2023*, 1–24.
30. Guo, T.; Han, Y.; Feng, C. A Survey on Attack and Defense of Block-chain System. *J. Softw.* **2021**, *32*, 1495–1525. [CrossRef]
31. Ilyas, B.; Kumar, A.; Setitra, M.A.; Bensalem, Z.A.; Lei, H. Prevention of DDoS Attacks Using an Optimized Deep Learning Approach in Blockchain Technology. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4729. [CrossRef]
32. Yakubu, B.M.; Khan, M.I.; Khan, A.; Jabeen, F.; Jeon, G. Blockchain-Based DDoS Attack Mitigation Protocol for Device-to-Device Interaction in Smart Home. *Digit. Commun. Netw.* **2023**, *9*, 383–392. [CrossRef]
33. Houda, Z.A.E.; Hafid, A.S.; Khoukhi, L. MiTFed: A Privacy-Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2023**, *2023*, 1985–2001. [CrossRef]
34. Jmal, R.; Ghabri, W.; Guesmi, R.; Alshammari, B.M.; Alshammari, A.S.; Alsaif, H. Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks. *Appl. Sci.* **2023**, *13*, 4953. [CrossRef]
35. Li, Q.; Huang, H.; Li, R.; Lv, J.; Yuan, Z.; Ma, L.; Han, Y.; Jiang, Y. A comprehensive survey on DDoS defense systems: New trends and challenges. *Comput. Netw.* **2023**, *233*, 109895. [CrossRef]
36. Zheng, R.; Ying, C.; Shao, J.; Wei, G.; Yan, H.; Kong, J.; Ren, Y.; Zhang, H.; Hou, W. New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defence Cost. In *Network and System Security*; Liu, J.K., Huang, X., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; Volume 11928, pp. 567–580. [CrossRef]
37. Chaganti, R.; Boppana, R.V.; Ravi, V.; Munir, K.; Almutairi, M.; Rustam, F.; Lee, E.; Ashraf, I. A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges. *IEEE Access* **2023**, *10*, 96538–96555. [CrossRef]
38. Guo, W.; Xu, J.; Pei, Y.; Yin, L.; Jiang, C.; Ge, N. A Distributed Collaborative Entrance Defense Framework Against DDoS Attacks on Satellite Internet. *IEEE Internet Things J.***2022**, *9*, 15497–15510. [CrossRef]
39. Wang, C.; Chu, X.; Qin, Y. Dissecting Mining Pools of Bitcoin Network: Measurement, Analysis and Modeling. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 398–412. [CrossRef]
40. Sood, A. DDOS Attacks Against Bitcoin Mining Pools: A New Game-Theoretic Analysis With Defense Cost. In Proceedings of the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 12–13 May 2023; pp. 2398–2402. [CrossRef]
41. Kesavan, R.; Pitchai, K.M. Modeling and Simulation of Selfish Mining Attacks in Blockchain Network using Evolutionary Game Theory. In Proceedings of the 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2–4 February 2023; pp. 1016–1021. [CrossRef]
42. Mighan, S.N.; Mišić, J.; Mišić, V.B.; Chang, X. An In-Depth Look at Forking-Based Attacks in Ethereum with PoW Consensus. *IEEE Trans. Netw. Serv. Manag.* **2023**, *2023*, 1–11. [CrossRef]
43. Sigmund, K.; Nowak, M.A. Evolutionary game theory. *Curr. Biol.* **1999**, *9*, 503–505. [CrossRef] [PubMed]
44. Hofbauer, J.; Sigmund, K. Evolutionary Game Dynamics. *Bull. Am. Math. Soc.* **2003**, *40*, 479–519. [CrossRef]
45. Ye, M.; Han, Q.-L.; Ding, L.; Xu, S. Distributed Nash Equilibrium Seeking in Games With Partial Decision Information: A Survey. *Proc. IEEE* **2023**, *111*, 140–157. [CrossRef]
46. Facchinei, F.; Kanzow, C. Generalized Nash equilibrium problems. *Ann. Oper. Res.* **2007**, *5*, 173–210. [CrossRef]