electronics

MDPI

Article

A Repeated Game-Based Distributed Denial of Service Attacks Mitigation Method for Mining Pools

Xiao Liu [1], Zhao Huang [2,*], Quan Wang [1], Yin Chen [3] and Yuan Cao [4]

[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.)
[2] Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China
[3] Graduate School of Media and Governance, Reitaku University, Kashiwa 277-8686, Japan; ychen@reitaku-u.ac.jp
[4] College of Internet of Things Engineering, Hohai University, Changzhou 213022, China; caoyuan0908@gmail.com
* Correspondence: z_huang@xidian.edu.cn; Tel.: +86-187-9261-0378

Abstract: A Distributed Denial of Service (DDoS) attack is a prevalent issue in the blockchain network layer, causing significant revenue loss for honest mining pools. This paper introduces a novel method, the Repeated Game-based DDoS attack mitigation (RGD), to address this problem. Unlike traditional methods such as game theory and machine learning-based detection, the RGD method can effectively reflect the changes in mining revenue and strategies under different network-strength environments. In particular, we abstract the problem of DDoS mining pool revenue loss into a game revenue model and propose the subgame perfect equilibrium (SPE) approach to solve the optimal payoffs and pool strategies in various network environments. Furthermore, we address the returns of mining pools in an infinitely repeated game environment using the Two-Stage Repeated Game (TSRG) method, where the strategy varies with different network environments. The Matlab experimental simulation results indicate that as the network environment improves, the optimal mining strategies of mining pools are gradually shifting from honest strategies to launching DDoS attacks against each other. The RGD method can effectively represent the impact of changes in the network environment on the mining pool's strategy selection and optimal revenue. Consequently, with the changing network environment, the optimal revenue of the mining pool only increases by 10% of the revenue loss during a DDoS attack.

Keywords: blockchain network; DDoS attack; subgame perfect equilibrium; two-stage repeated game; mining pools; PoW security

check for updates

Citation: Liu, X.; Huang, Z.; Wang, Q.; Chen, Y.; Cao, Y. A Repeated Game-Based Distributed Denial of Service Attacks Mitigation Method for Mining Pools. *Electronics* **2024**, *13*, 398. https://doi.org/10.3390/electronics13020398

Academic Editor: Mehdi Sookhak

Received: 27 November 2023
Revised: 13 January 2024
Accepted: 16 January 2024
Published: 18 January 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The consensus algorithm [1], specifically the Proof of Work (PoW) [2], is a cornerstone of blockchain technology, ensuring data consistency and system consensus [3]. However, PoW's reliance on computational power exposes blockchain to security risks, including selfish mining (SM) attacks [4], block withholding (BWH) attacks [5], and Distributed Denial of Service (DDoS) attacks [6]. SM attacks gain additional revenue by creating redundant private chains in addition to the public chain [7]. BWH attacks generate illegal revenue by sending spy miner attacks to honest mining pools [8]. However, the most common attack among these attacks is the DDoS attack. DDoS attacks disrupt connectivity between honest mining pools and mining websites, leading to significant revenue loss [9]. Addressing the vulnerability of PoW blockchains to DDoS attacks is a pressing issue in the field [10].

Recent research has proposed three types of solutions to mitigate the impact of DDoS attacks on blockchain mining pools: detection methods, static game models, and dynamic game models [11]. Detection methods are utilized to identify and differentiate abnormal traffic within the blockchain network [12]. This is achieved through the use of classification

methods, such as machine learning, which can predict the presence of DDoS attacks in advance. However, this approach does not address the problem of reduced revenue from mining pools after a DDoS attack has already occurred. To address this issue, the static approach determines the optimal strategy of the mining pool through a finite number of games and a Nash equilibrium, keeping the network environment constant [13]. This approach mitigates the problem of diminishing returns, but it cannot adapt to complex network environments. To further address the drawbacks of static games, the dynamic game method, which adapts and evolves to find the optimal strategy for resisting DDoS attacks in various network environments, has been particularly effective [14]. However, it has limitations in reflecting the impact of network environment changes on mining pool income and showcasing the trend of changing strategies under attack [15]. Therefore, a repeated game approach is now being considered to address these issues [16,17].

To solve these issues, we propose an RGD method for mining pools. We have abstracted the problem of reduced revenue from a DDoS attack on a mining pool in a blockchain network into a revenue model for two mining pools. After that, we solve the game model using an SPE method and obtain the optimal strategy for mining pools encountering DDoS attacks in different network environments. Finally, according to the optimal strategy obtained by SPE, we solve the specific mining probability and optimal revenue under the condition that the mining pool chooses the mixed strategy by a TSRG method. A Matlab simulation experiment shows that the optimal strategy of the mining pool gradually shifts to a DDoS attack strategy as the network condition becomes better. Meanwhile, the mining revenue of the mining pool and the probability of hybrid mining will first increase and then decrease as the network situation improves.

- To the best of our knowledge, this paper is the first to use a repeat game method to study the selection of the profitable optimal strategy for mining pools that encounter DDoS attacks.
- We implement a game revenue model for a mining pool in a blockchain network environment that takes into account DDoS attacks.
- We employ the SPE approach to determine the mining chances and earnings of the mining pool's pure strategy to withstand DDoS attacks in various network settings. Additionally, we employ the TSRG technique to examine the mining probability and the trend of the maximum revenue in the network environment where the optimal strategy of the mining pool is mixed.
- The experimental results demonstrate that as network conditions improve, mining pools shift their optimal strategy from honest mining to launching DDoS attacks. To be clear, compared to static and evolutionary games, our RGD approach better illustrates how changes in the network environment affect mining strategies and the maximum profit of the mining pool.

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

2. Research Background

2.1. DDoS Attacks in Blockchain Networks

In blockchain, DDoS attacks are one of the most common mining attacks [18]. DDoS attacks are mainly launched through the blockchain network to launch attacks on honest mining pools for illegal gains [19]. The principle of DDoS attacks in blockchain networks is shown in Figure 1. We can see from Figure 1 that the steps of a DDoS attack are as follows [19]:

(1). Malicious nodes control peers in the blockchain over the network.

(2). Nodes in a blockchain network are connected. DDoS attacks are transmitted over the network to the victim.

(3). Honest mining pools are cut off from mining sites after a DDoS attack and the victims are unable to continue mining.

(4). After disconnecting the honest mining pools from the mining sites, the attackers use the malicious nodes under their control to launch DDoS attacks against the victims. The attacked victims lose a portion of their previous honest mining revenue. This portion of the earnings is transferred to the attackers through the blockchain network, and the attackers receive the proceeds of the attack.

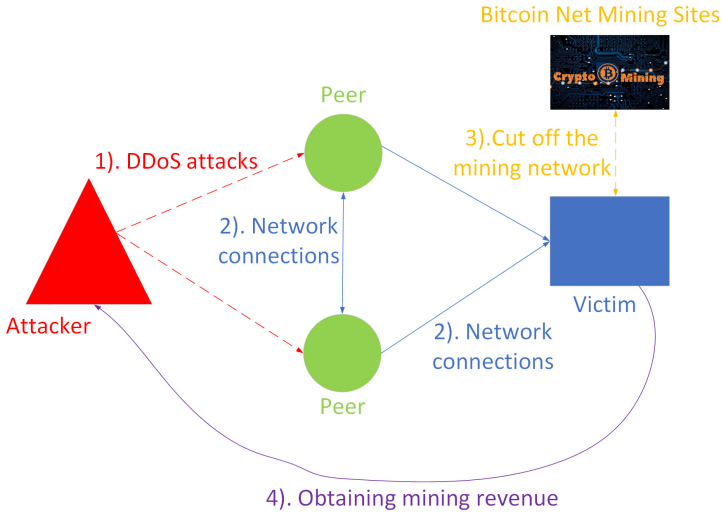

Figure 1. Diagram of a DDoS attack.

From the DDoS attack principle, we can conclude that a DDoS attack uses networks to control multiple malicious nodes that send excessive network requests or traffic to disrupt the connection between honest mining pools and mining sites. Then, honest mining pools lose a portion of their mining revenue due to DDoS attacks [20]. Furthermore, DDoS attacks will cause huge revenue losses to mining pools through the network and also make pools unable to continue mining for revenue [21]. Therefore, how to effectively solve the problem of the mining pool in the blockchain network suffering from DDoS attack mining revenue reduction is one of the important focus issues of the academic community.

2.2. DDoS Attack Detection Methods

Currently, there is a significant amount of research using machine learning-based methods to detect the presence of DDoS attacks in advance by detecting the excessive number of network requests or abnormal traffic in the blockchain network. This kind of detection method can detect the existence of DDoS attacks in the blockchain network in advance so that the revenue loss caused by DDoS attacks on honest mining pools can be avoided in advance. Mishra et al. [22] proposed a hybrid decision tree method based on machine learning and blockchain to prevent and detect the presence of DDoS attacks by detecting abnormal traffic and delays in blockchain networks. Truong et al. [23] designed a collaborative intrusion detection system based on blockchain and federated learning. The system used a federated learning model to identify suspicious traffic that does not match normal traffic and presented it as evidence of an intrusion into smart contracts for verification and detection of DDoS attacks in the blockchain network. Jian et al. [24] proposed a framework based on information theory and blockchain to defend against distributed denial-of-service (DDoS) attacks in software-defined industrial Internet of Things (IoT). This framework detects and mitigates illegal traffic in the blockchain by using a combination of joint entropy and conditional entropy methods to detect DDoS attacks in blockchain networks. Ilyas et al. [25] implemented an approach based on blockchain technology and optimized deep learning to detect and prevent DDoS attacks in blockchain. The approach using smart contracts identifies DDoS attacks via network traffic, network

request volume, and packet generation frequency. The technique also applies the proposed predatory raptor optimization algorithm to adjust the weights of deep neural network (DNN) classifiers, resulting in improved detection accuracy and reduced training loss.

Research on DDoS detection methods in recent years is summarized in Table 1. Furthermore, these studies are also flawed in that they do not address the problem of reduced returns from mining pools. This shortcoming needs to be addressed in a DDoS attack mitigation approach. Next, we need to summarize and analyze the research on reducing the benefits of mining pools.

Table 1. Summary of DDoS Attack Detection Methods in Blockchain.

Reference	Purpose	Mechanism and Solution	Method	Defect
[22]	Defend against DDoS attacks in advance	Use decision tree methods to detect and differentiate traffic to predict DDoS attacks	Decision tree	Mining pool revenue mitigation cannot be solved.
[23]	Detecting DDoS attacks in federated learning	Use federated learning models and smart contracts to detect DDoS attacks	Federated learning models and smart contracts verification	The detection method is only applicable to the federal learning domain and is not universal.
[24]	Detecting DDoS attacks in the Industrial IoT	Using a combination of joint entropy and conditional entropy methods to detect DDoS Attacks	Entropy methods	Too complex to detect anomalous traffic using the entropy methods.
[25]	Detect and prevent DDoS attacks by optimized deep learning	Enhanced Raptor optimization algorithm identifies network traffic, network request volume, and other parameters to predict DDoS attacks	Enhanced Raptor optimization algorithm	The effectiveness of the Raptor method depends on the quality of the data. If the data is incomplete or noisy, the results may not be accurate.

2.3. DDoS Attack Mitigation Methods

The study of how to decrease income loss and prevent DDoS attacks in blockchain networks employs game theory to implement a model for determining the best mining strategy. This method aims to reduce revenue lost from DDoS attacks on mining pools. Currently, research in this field is primarily split between static game and dynamic evolutionary game methods.

Some recent research investigates DDoS attacks in blockchains, utilizing a static game approach. Table 2 shows the specific research summary. Then, we analyze the work of static methods in detail through Table 2. Johnson et al. [26] used static game theory to build a revenue model and analyze the motivation and impact of DDoS attacks between Bitcoin mining pools. This method solves the Nash equilibrium strategy of mining pools and discusses the impact of different investment strategies and attack effects on mining revenues. Saad et al. [27] proposed a DDoS attack mitigation method based on a static game for the Bitcoin storage pool. This method effectively solves the problem of DDoS attacks using a large number of unconfirmed micro-transactions to occupy the memory pool space and force legitimate users to pay higher mining fees through a fee-based and age-based memory pool design scheme. Alzahrani et al. [28] proposed a blockchain consensus protocol based on static game theory and randomness. The protocol effectively protects against DDoS attacks by designing a novel reward and punishment mechanism to incentivize honest behavior in mining pools. KACI et al. [29] presented a blockchain trust model based on a static game. The model manages the reputation of miners on the blockchain through a job market signaling game model that incentivizes miners to mine honestly and penalizes malicious miners while protecting the mining pool from DDoS attacks by malicious miners.

Table 2. Summary of static methods for DDoS revenue mitigation.

Reference	Purpose	Mechanism and Solution	Method	Defect
[26]	Static game revenue mitigation model of DDoS attacks	Solving the optimal mining pool strategy using static game and Nash equilibrium methods	Static game method	Cannot reflect the changing trend of the optimal strategy over time.
[27]	Using a static game method to ease the transaction cost	Reduce DDoS-induced increases in transaction fees	Static game method	Cannot mitigate the loss of mining pool revenue.
[28]	Alleviating the problem of reduced benefits from DDoS attacks	Encourages honest behavior in mining pools through static game modeling and reward mechanisms	Static game	Over-reliance on honest behavior and reward mechanisms.
[29]	Improve the reputation of honest mining pools to reduce revenue	Manage miners' reputations using the job market signal game model	Job market signal game model	Reputation mechanism cannot ensure the authenticity and reliability of miners' information transmission.

Some research employs a dynamic game approach to address the issue of diminished returns for mining pools and miners caused by DDoS attacks. Table 3 summarizes the specific dynamic methods. Then, we elaborate on the research content of Table 3. Huang et al. [30] established a profit model of miners' resistance to DDoS attacks by using the dynamic evolutionary game method and solved the optimal mining strategy of miners in different network environments by using the Friedman method. Mirkin et al. [31] implemented an Incentive-Based Denial of Service (IBDoS) attack using a blockchain reward mechanism to disrupt the operation of a PoW-based cryptocurrency system using a dynamic game approach. Wu et al. [32] used a stochastic dynamic game model and Q-learning algorithm to analyze and optimize DDoS attack strategies among Bitcoin mining pools. This approach can effectively mitigate the impact of DDoS attacks on mining pool revenue and miner migration. Sharma et al. [33] proposed a method based on an adaptive dynamic non-cooperative game to help mining pools effectively defend against DDoS attacks.

Table 3. Summary of dynamic methods for DDoS revenue mitigation.

Reference	Purpose	Mechanism and Solution	Method	Defect
[30]	Alleviates the problem of reduced revenue for miners under different networks	Modeling and solving optimal mining strategies using dynamic evolution and dynamic replication equations	Dynamic evolution game method	The issue of relief from pool revenues has not been addressed
[31]	Implement incentive-based DDoS attacks	Use a dynamic gaming approach to mitigate revenue loss from this new DDoS-based attack	Dynamic gaming approach	Neglecting the security analysis and research of the original DDoS attack threat
[32]	Mitigate DDoS impact on pool revenue and miner migration	Optimizing mining pool returns with stochastic dynamic game and Q-learning algorithm	Stochastic dynamic game and Q-learning algorithm	Exploring the optimal strategy using the Q-learning method is inefficient
[33]	Prevent and defend DDoS attacks	Adaptive dynamic non-cooperative game mitigates DDoS attacks	Dynamic non-cooperative game	Non-cooperative game assumes the conditions are too hard

2.4. Challenges in Current Researches

These methods can detect DDoS attacks or mitigate DDoS attacks in advance to a certain extent. However, these methods have some limitations and defects. First, DDoS

detection methods can only detect the existence of DDoS attacks in advance. They cannot effectively mitigate the reduction in mining revenue from mining pools after a DDoS attack on a blockchain network. Second, the static game method can only fulfill the optimal strategy derived by mining pools against DDoS attacks within a single network environment. However, it cannot cater to the demands of an effective network environment in a complex and changing network environment. To illustrate this problem, we offer two DDoS revenue mitigation scenarios for complex environments. These two cases are illustrated in Figure 2. The first scenario in Figure 2a is mainly when a malicious mining pool attacks an honest mining pool through a blockchain network for illegal rewards. In this scenario, the network topology is not complicated, but the problems in the network environment will constantly change. How to model DDoS attack mitigation according to different intensity network environments is a complex problem. The second complex network situation in Figure 2b is that the malicious mining pool controls multiple puppet nodes in different network environments to attack the honest mining pool. The malicious mining pool is connected to puppet nodes to launch DDoS attacks against the honest mining pool to generate revenue. The network topology is complex. It is also a difficult problem to study how to mitigate the benefits of DDoS mining pools according to the change in the intensity of the network environment and the number of puppet nodes. Third, dynamic evolution and stochastic games can assist in implementing mining strategies that optimize the gains of mining pools against DDoS attacks within various network environments. Nevertheless, these techniques cannot address the effects and quantification of changing network conditions on the optimal game strategy and the optimal mining revenue.

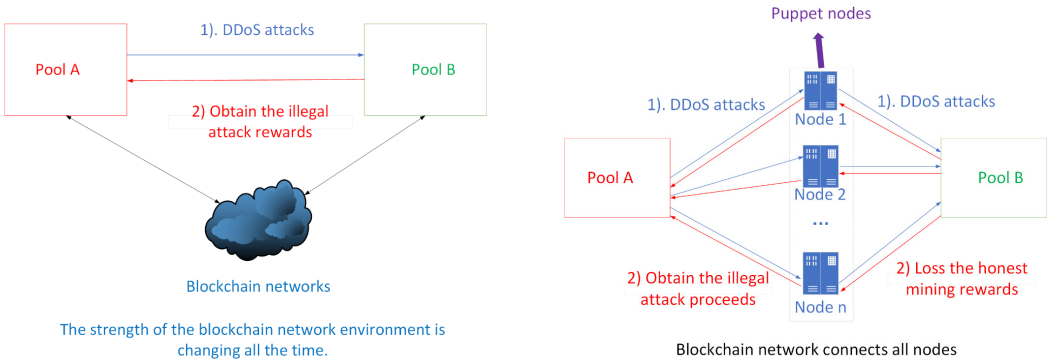

Figure 2. DDOS attacks in complex network situations. (**a**) Situation 1. (**b**) Situation 2.

To address these issues, we propose an RGD mitigation method. In particular, we construct a game revenue model for mining pools suffering DDoS attacks. Then, we propose an SPE strategy to solve the optimal mining strategy and revenue variation of this model under different network environments. Finally, we utilize a TSRG approach to solve for the probability of occurrence of mixed strategies and the trend of optimal mining revenue with network environment coefficients for mining pools defending against DDoS attacks in a moderate network environment. We demonstrate the correctness and effectiveness of our RGD approach by comparing static, dynamic evolutionary, and repeated game experiments.

3. The Proposed Repeated Theory Model and Solutions for Mining Pools against DDoS Attacks

3.1. Problem Hypotheses and Modeling

This section aims to model the problem of revenue reduction in scenarios where mining pools encounter DDoS attacks in the blockchain. Table 4 provides a detailed introduction to the modeling parameters. Specific problem abstractions and parameter assumptions are described below.

Table 4. DDoS attack modeling parameters for mining pools.

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 mining pool.
a	When pools mine honestly with the same mining pool, the pool manager gives the reward to the honest pool.
c	When a malicious pool launches a DDoS attack, the attacker is punished by the pool manager.
w	Network environment coefficient.
p_1	The probability of honest mining of a mining pool under mixed probability.
p_2	Mining strategies for repeated game mining pools.
δ	Discount factor for mining in an infinite repeated game mining pool.
R_B	Optimal returns for mining pools under harsh networks.
R_M	Optimal returns for mining pools under medium networks.
R_G	Optimal returns for mining pools under good networks.

The purpose of this section is to provide a detailed analysis of the revenue mitigation problem of DDoS mining pools. To achieve this, we will combine the parameter introduction table in Table 4 with previous related work [34]. Also, we will elaborate on the specific assumptions, analysis, and parameter introduction required for this problem.

(1). Pool A and pool B have the same computing power, and the mining revenue from honest mining is R. The value of this mining revenue R is $R > 0$.

(2). The gain of a certain mining pool from DDoS attacks is wd, and the loss of the same mining pool from DDoS attacks is also wd. w indicates the network environment coefficient. The value range is $0 \leq w \leq 1$. The $w = 0$ indicates that the network environment strength is 0 and the network is down and disconnected. This means that the network environment is offline. At this point, the value of the illegal gain from the malicious mining pool launching the attack is 0. $w = 1$ disconnection. A malicious mining pool launching a DDoS attack would obtain a complete gain independent of network strength. Therefore, we will refer to this case of $w = 1$ as the ideal case for the network. This additionally indicates that the blockchain network is smooth and there is no network block and d represents the illegal proceeds of DDoS attacks launched by mining pools under ideal network conditions ($w = 1$).

(3). The pool manager rewards honest mining pools with a value of a and punishes attacking pools with a value of c. The values of a and c are $a > 0$ and $c > 0$.

(4). The presence of miners and the migration of miners to choose different mining pools are not considered in this paper.

(5). To simplify the model, we assume that all DDoS attacks in this paper originate from mining pools A and B. The attack scenarios for these pools differ based on whether or not DDoS attacks are launched by them.

After explaining the hypothesis, abstraction, and parameters of the problem, this paper will introduce the game payoff model through a specific attack scenario. We need to analyze the profits of mining pools in the blockchain network environment through a DDoS attack scenario. Our abstractions, assumptions, and modeling of the problem are the same as in previous work [34]. The specific attack scenario is shown in Figure 3. As can be seen from Figure 3, we consider the following DDoS attack scenario. In this attack scenario, we consider that only two mining pools A and B in the blockchain network have the same computing power. Pool A and pool B both obtain rewards of R for honest mining. Mining pool A launches DDoS attacks on mining pool B through the network to obtain illegal profits. The illegal reward when mining pool A launches a DDoS attack on mining pool B is wd, where w is the network environment coefficient and its value is $0 \leq w \leq 1$ when $w = 1$, the network is in an ideal state, and when $w = 0$, the network is disconnected. Similarly,

the loss of revenue from an attack on pool B is also wd. The mining pool manager gives a penalty of c to the mining pool A that launched the attack. The pool manager rewards honest pool B with a for honest mining. In this DDoS attack scenario, the mining income of mining pool A is $R + wd - c$, and the income of pool B is $R - wd + a$. Table 1 describes the parameters of the model used in this paper in detail. In Table 4, we describe in detail how this problem is abstracted into a game payoff model. Specific problem abstractions and parameter assumptions are described below.

We use the above parameter settings to analyze four attack scenarios similar to the DDoS attack scenario in Figure 3. These DDoS attack scenarios mainly divide the entire scenario into four categories based on the specific attack of the mining pool in the blockchain. The four attack scenarios are (Honest mining (H), Honest mining (H)), (Honest mining(H), DDoS attacks(D)), (DDoS attacks(D), Honest mining(H)), (DDoS attacks(D), DDoS attacks(D)). (H, H) means that pool A and pool B are honestly mining in blockchain networks. (H, D) means that mining pool A is honest mining in the blockchain network, while mining pool B launches DDoS attacks. (D, H) means that mining pool B is honest mining in a blockchain network, while mining pool A launches DDoS attacks. (D, D) means that both pool A and pool B launch DDoS attacks against each other. Based on our previous work [34], we describe the payoff matrix analysis of the four attacks as follows:

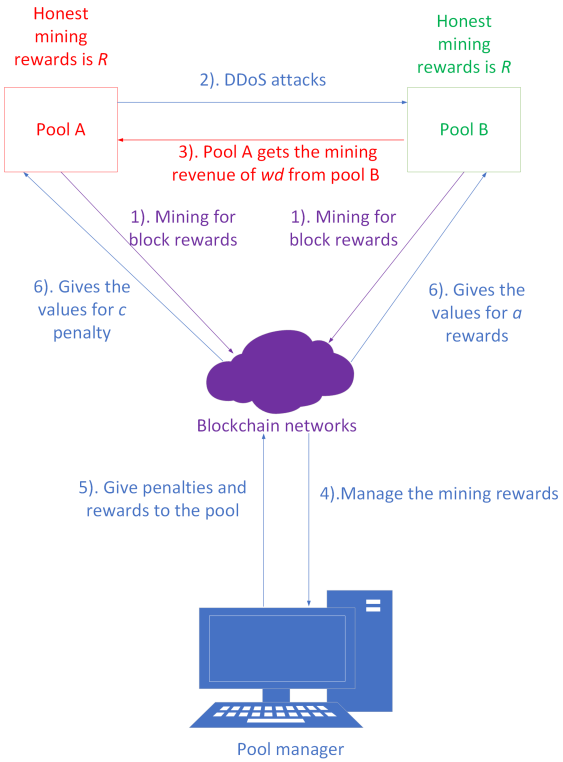

Figure 3. A scenario of a DDoS attack by mining pools in a blockchain network.

(1). (H, H) means that pool A and pool B are both mining honestly, so they both obtain R. This DDoS attack scenario is illustrated in Figure 4.

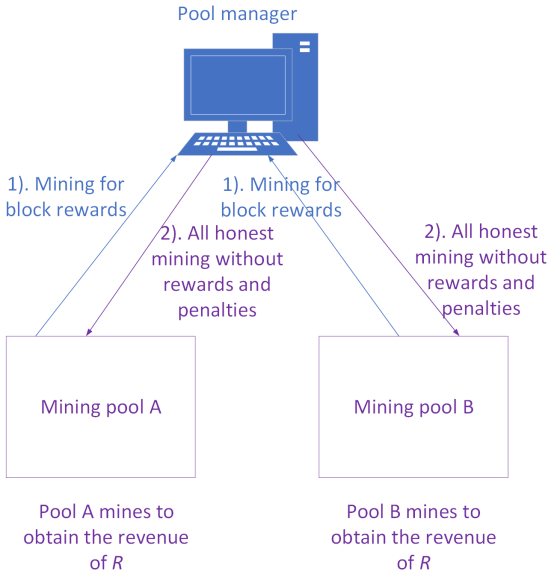

Figure 4. A scenario where both pool A and pool B mine honestly.

(2). (H, D) means that pool A is honestly mining for rewards, while pool B launches DDoS attacks for illegal rewards. The payoff of pool A and pool B mining honestly is R. The gain from a DDoS attack on pool B is wd, and the loss from an attack on pool A is wd. The pool manager gives pool A a reward of a and pool B a punishment of c. Therefore, the revenue of mining pool A is $R - wd + a$, and the mining revenue of mining pool B is $R + wd - c$. This DDoS attack scenario is illustrated in Figure 5.

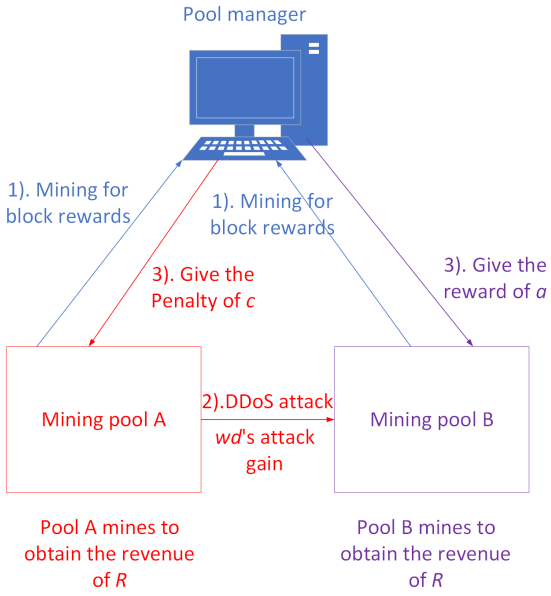

Figure 5. A scenario in which mining pool A is mining honestly and mining pool B is launching DDoS attacks.

(3). (D, H) means that mining pool A launches a DDoS attack on mining pool B, while mining pool B mines honestly. Mining pool A launches DDoS attacks on mining pool B to gain gains from wd, while mining pool B suffers losses from wd. The pool manager gives pool B a reward of a and pool A a punishment of c. Therefore, the revenue of mining pool A is $R + wd - c$, and the mining revenue of pool B is $R - wd + a$. This DDoS attack scenario is illustrated in Figure 6.

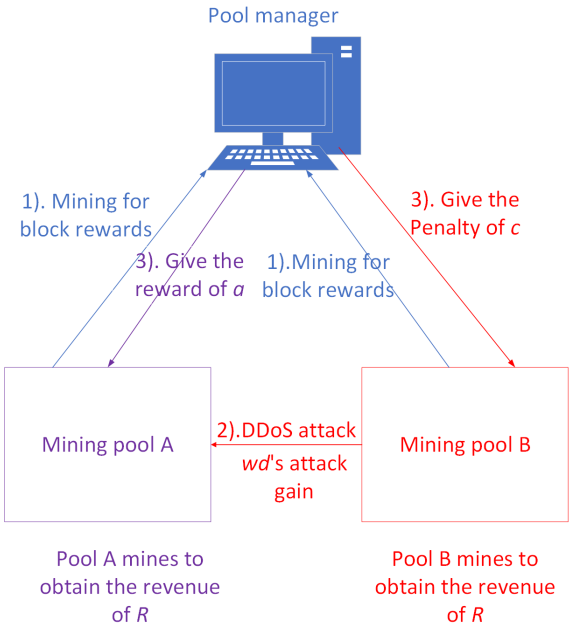

Figure 6. A scenario in which mining pool B is mining honestly and mining pool A is launching DDoS attacks.

(4). (D, D) means that pool A and pool B launch DDoS attacks against each other. Since pool A and pool B have the same computing power, the loss of DDoS attacks launched against each other is wd, and the attack income is also wd. Pool A or pool B attack each other and the sum of the attack gains and losses is 0. Pool A and pool B both earn R from honest mining. The pool manager assigns a penalty of c to both pool A and pool B for attacking each other. Therefore, the mining revenue of both pool A and pool B is $R - c$. This DDoS attack scenario is illustrated in Figure 7.

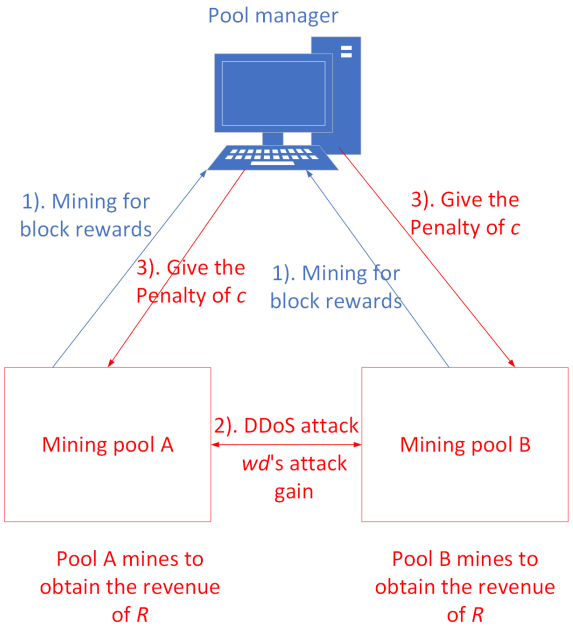

Figure 7. A scenario where mining pool A and mining pool B launch DDoS attacks against each other.

From the above four attack scenarios, we can obtain the mining benefits of mining pools A and B in this scenario as described in Table 5.

Table 5. The revenue of mining pools A and B when attacked by DDoS attacks (Table 5 model is obtained from [34]).

Pool A \ Pool B	Honest Mining (H)	DDoS Attacks (D)
Honest mining (H)	(R, R)	$(R - wd + a, R + wd - c)$
DDoS attacks (D)	$(R + wd - c, R - wd + a)$	$(R - c, R - c)$

After obtaining the game payoff Table 5 of our previous work [34], we solve the optimal mining strategy for the mining pool suffering DDoS attacks in different network environments. The optimal mining strategies we previously obtained through an evolutionary game method [34] can obtain the optimal strategies in different network environments after multiple game iterations. However, this evolutionary game approach cannot effectively distinguish how mining pools can effectively defend against DDoS attacks in the case of finite and infinite subgames. Also, this evolutionary game approach cannot concretely realize the optimal strategies of mining pools under the change in network environment, and the trend of returns and mixed strategies with the change in network environment. Therefore, we need to use the repeated game method in the following to realize the optimal mining strategy, revenue, and mixed strategy changes of the mining pool to resist DDoS attacks under finite and infinite games.

3.2. Optimal Mining Strategy for Finite Repetition Games

In the previous work [34], we completed the construction of the revenue model and income statement of the DDoS attack on mining pool A and mining pool B. We need to solve the optimal mining strategy of resisting DDoS attacks of mining pools' repeated games when the number of games is limited, and the trend of mining probability of optimal returns and mixed strategies changing with a network environment w in this section. The goal of this section is to address the changing network environment range w through the subgame's perfect equilibrium strategy in the finite repetition game. Then, we determine the most profitable way to mine when using the pure strategy, considering the varying conditions of different network environments. Finally, we use the expected returns of mining pools A and B to solve the optimal strategy of the mining pools, which is the changing trend of the optimal return and mining probability under the mixed strategy.

We analyze the impact of the network environment fetch range on the selection of optimal policy choices for mining pools to defend against DDoS attacks using the payoff table in Table 5. We divide the value range of network environment coefficient w into three parts by the attack strategy of pool A and pool B by the SPE method [35]. We discuss the values of different network environments, the optimal strategy, and the utility of mining pools in three cases. Each network situation is a subgame. The perfect equilibrium strategy to solve the subgame is to solve the optimal strategy and payoff of the mining pool. Also, we solve the value of w and solve the optimal mining strategy, honest mining probability, and optimal mining revenue under different values of w. The analysis and derivation presented below reveal the precise network environment coefficients, optimal strategies for diverse network environments, mining probabilities, and optimal returns. References to subgame perfect equilibrium theory are used in the computation of our Equations ([35,36]).

(1). From Table 5, we can conclude that the expected returns of honest mining in both pool A and pool B are R when the optimal strategy is (H, H). If pool A launches a DDoS attack and pool B is still honestly mining, then the mining revenue of pool A is equal to $R + wd - a$. The anti-DDoS strategy of the mining pool is (D, H). We can obtain that if mining pool A selects the honest mining strategy, the (H, H) strategy generates a higher return compared to the (D, H) strategy. In this scenario, it is clear that the honest mining revenue is preferable to the income obtained from the (D, H) strategy, as the latter yields smaller returns compared to the (H, H) scenario. As a result, mining pool A will choose honest mining as the most favorable option. Similarly, if mining pool B selects the (H, D) strategy with lower returns than (H, H), pool B will opt for honest mining

with the best returns. Under both (D, H) and (H, D) strategies, pool A and pool B receive $R + wd - c$. Moreover. we compare the value of these two types of profits with the profit R from the (H, H) strategy to determine the network environment coefficient in this situation. Finally, we examine the scope of the network environment coefficient w in this case using Equation (1).

$$\begin{aligned} R &< R + w * d - c \\ &\leftrightarrow wd < c \\ &\leftrightarrow w < \frac{c}{d} \end{aligned} \tag{1}$$

According to Equation (1) and the game model in Section 3, we can obtain that the value of a network environment coefficient w for mining pool A and B to choose (H, H) strategy is $0 \leq w < \frac{c}{d}$. By analyzing Equation (1), we know that in this attack environment, the value of network environment w is relatively small. This means that in a harsh network environment, mining pool A and mining pool B choose the honest mining strategy to make the best profit. Under the best strategy p_2 for the harsh network environment (H, H), the optimal returns R_B of mining pool A and mining pool B are both R. R_B means the mining rewards under a bad network condition.

(2). If the return of the mining strategy (H, D) chosen by mining pool A is lower than the return of the mining strategy (D, D), then mining pool A will choose to launch a DDoS attack for maximum profit. If mining pool B earns more profit in strategy (D, H) than in strategy (D, D), mining pool B will also choose a DDoS attack strategy. Both pool A and pool B receive $R - wd + a$ in the (H, D) and (D, H) strategies. The revenue of mining pools A and B are compared with the benefits $R - c$ obtained using strategy (D, D). Subsequently, the value of the network environment coefficient w for this scenario is calculated, as outlined in Equation (2).

$$\begin{aligned} R - w * d + a &< R - c \\ &\leftrightarrow -wd + a < -c \\ &\leftrightarrow w > \frac{a + c}{d} \end{aligned} \tag{2}$$

From Equation (2), we can conclude that the right side of the inequality is the optimal return for a given mining pool as network conditions improve, and the left side of the inequality is the value that is closest to the optimal return. A range of values for the network environment goodness factor is obtained by solving the inequality in this manner. According to Equation (2) and the game model in Section 3, we can determine the network environment coefficient w for mining pool A and mining pool B to select an optimal DDoS attack strategy for maximum profit, with a requirement that $\frac{a+c}{d} < w \leq 1$. According to the value of w in Equation (2), we can obtain that w is in a situation where the value is relatively large, indicating that both mining pool A and mining pool B will choose the (D, D) strategy to obtain the optimal returns under a good network condition. We define R_G as the best revenue in good networks for pools. Therefore, mining pools choose P_2 as the (D, D) strategy that is profitably optimal. Also, pool A and pool B both have an optimal return R_G of $R - c$.

(3). When the value of the network environment coefficient w is $\frac{c}{d} < w < \frac{a+c}{d}$, mining pools A and B have the best profit when multiple strategy choices exist simultaneously, called a mixed strategy state. Then, we know that the network environment is currently in a medium environment from the value of w. We must calculate the probability of honest mining and optimal mining returns using a mixed strategy when the mining pool is under a DDoS attack in a mid-network environment. Also, we assume that the probability of honest mining using a pool mix strategy in our model is p_1. Then, both pool A and pool B are mining pools with equivalent computing power, resulting in an identical honest mining probability of p_1. The predicted gain for mining honestly in a mining pool equals the predicted gain for carrying out a DDoS attack. Based on the equivalent expected payout

analysis, we present the probability p_1 for a mining pool to engage in honest mining under a mixed strategy utilizing Equation (3).

$$\begin{aligned} p_1 * R + (1 - p_1) * (R - wd + a) &= p_1 * (R + wd - c) + (1 - p_1) * (R - c) \\ 0 &= p_1 * (wd - c) + (1 - p_1) * (wd - a - c) \\ 0 &= (wd - a - c) + a * p_1 \\ p_1 &= \frac{a + c - wd}{a} \end{aligned} \tag{3}$$

From Equation (3), we can see that the probability of honest mining is $p_1 = \frac{a+c-wd}{a}$ when pool A and pool B select a mixed strategy for p_2 in a medium network environment. In this scenario, a mining pool selects the mixed strategy that yields the highest profit by using the probability p_1 for honest mining. Based on the likelihood of mining (p_1), we calculate the anticipated income (R_M) for pool A and pool B using Equation (4) when applying a mixed strategy.

$$\begin{aligned} R_M &= p_1^2 * R + p_1(1 - p_1)(R - wd + a) + (1 - p_1)p_1(R + wd - c) + (1 - p_1)^2 * (R - c) \\ &= p_1^2 R + p_1(1 - p_1)(2R + a - c) + (1 - p_1)^2 * (R - c) \\ &= -ap_1^2 + (c + a)p_1 + R - c \end{aligned} \tag{4}$$

From Equation (4), we can conclude that the first term in the sum is the gain from mining pools A and B mining honestly at the same time, and the second term is the gain from mining pool A mining honestly while mining pool B launches an attack. The third term is the gain from mining pool B mining honestly while mining pool A launches an attack. The fourth term is the benefit of both pools A and B attacking each other. We can obtain the mining probability $p_1 = \frac{a+c-wd}{a}$ for the mixed strategy from Equation (4) to each term. This suggests that the optimal mixing probability multiplied by the optimal gain for all attack scenarios is the optimal total gain for the medium network. Then, we substitute the specific expression of p_1 in Equation (3) to obtain the specific value R_M of the optimal return of the mixed strategy, as described in Equation (5).

$$\begin{aligned} R_M &= -ap_1^2 + (c + a)p_1 + R - c \\ &= -a * (\frac{a + c - wd}{a})^2 + (c + a) * (\frac{a + c - wd}{a}) + R - c \\ &= -\frac{(a + c - wd)^2}{a} + (c + a) * \frac{a + c - wd}{a} + R - c \\ &= \frac{-(a + c - wd)^2 + (c + a) * (a + c - wd)}{a} + R - c \end{aligned} \tag{5}$$

From Equation (5), we can conclude that the optimal mining revenue is R_M in the case where pool A and pool B defend against DDoS attacks by choosing a mixed strategy where $p_1 = \frac{a+c-wd}{a}$. From the value of R_M, we can obtain that its expression consists of only one variable parameter w. As the network environment coefficient w increases, the optimal return R_M of the hybrid strategy first increases to reach the extreme value and then decreases. Based on the above analysis and derivation, we obtained the SPE strategy and the returns of the mining pool in the finite repetition game. Then, our specific implementation of the SPE algorithm is shown in the description of Algorithm 1.

Through Algorithm 1, we can know the optimal mining revenue and strategy when mining pools resist DDoS attacks in a finite repeated game situation. We initialize the input parameters of the return R, the attack penalty c, the reward a, and the attack return d. Also, we have defined the optimal strategy $strategy_A$, $strategy_B$, returns $payoff_A$, $payoff_B$, and probability p_A, p_B of mixed mining for all three different SPE cases using the outputs of Algorithm 1. Line 1 of the pseudo-code initializes the variable parameter network environment coefficient $w(i)$ and gives $w(i)$ the value range $0 \leq w(i) \leq 1$. Also,

this line of pseudocode initializes the optimal mining strategies $strategy_A$, $strategy_B$, the optimal mining $payoff_A$, $payoff_B$, and the probability of mining with mixed strategies p_A, p_B for mining pool A and mining pool B. Lines 2 to 7 of the pseudocode determine the mining pool's optimal strategy and revenue against DDoS attacks in a harsh network environment, where 1 is the honest mining strategy. Lines 8 to 12 of the pseudocode derive the optimal strategy and revenue for mining pools in a good network environment, where 2 is a DDoS attack strategy. Lines 13 to 21 of the pseudo-code explain the mining probability and mining revenue in the case of an optimal mixed strategy. The number 3 represents the best profit for a mining pool to choose the mixed strategy.

Algorithm 1 DDoS Attack Mining Pool Optimal Policy Subgame Perfect Equilibrium Algorithm

Input: R, c, d, a
Output: $strategy_A, strategy_B, payoff_A, payoff_B, p_A, p_B.w(i)$
1: Initialize the value of $strategy_A$, $strategy_B$, $payoff_A$, $payoff_B$, p_A, p_B
2: **for** $i \leftarrow 1$ to length(w) **do**
3: **if** $w(i) > c/d$ **then**
4: $strategy_A(i) \leftarrow 1$
5: $strategy_B(i) \leftarrow 1$
6: $payoff_A(i) \leftarrow R$
7: $payoff_B(i) \leftarrow R$
8: **else if** $w(i) < \frac{c+a}{d}$ **then**
9: $strategy_A(i) \leftarrow 2$
10: $strategy_B(i) \leftarrow 2$
11: $payoff_A(i) \leftarrow R - c$
12: $payoff_B(i) \leftarrow R - c$
13: **else**
14: $strategy_A(i) \leftarrow 3$
15: $strategy_B(i) \leftarrow 3$
16: $payoff_A(i) \leftarrow \frac{-(a+c-w(i)*d)^2+(c+a)*(a+c-w(i)*d)}{a} + R - c$
17: $payoff_B(i) \leftarrow \frac{-(a+c-w(i)*d)^2+(c+a)*(a+c-w(i)*d)}{a} + R - c$
18: $p_A(i) \leftarrow \frac{c+a-(w(i)*d)}{a}$
19: $p_B(i) \leftarrow \frac{c+a-(w(i)*d)}{a}$
20: **end if**
21: **end for**

3.3. Optimal Mining Strategy for Infinite Repetition Games

In Section 3.2, we employ the SPE method to determine mining pools' optimal strategy and revenue, as well as a mixed strategy to counter DDoS attacks across varying network environments in finite repeated games. In this section, we will examine the solution and changing trends of the optimal strategy, revenue, and mixed equilibrium probability for the mining pool in the context of infinite repeated games. We divide the infinitely repeated games into three cases according to the different values of the network environment according to the SPE method. Also, we use the TSRG method to realize and solve the optimal strategies and returns of mining pools in three types of network environments [37]. Moreover, the initial step in TSRG involves utilizing the SPE method for finite repetitive games as outlined in Section 3.2. The subsequent stage of the repetitive game in TSRG involves solving for the change in mining pool strategy and revenue in an infinite repetitive game scenario. Based on three different network environments solved by the SPE method in the first-stage game in Section 3.2, we analyze the benefits and strategies of DDoS attacks on mining pools in the second-stage infinite repeated game using the TSRG method, assuming the global discount factor δ. We refer to the repeated game theory literature for formulas and theoretical analysis of infinite repeated games [37,38].

(1). If the value of the variable parameter w is $0 \leq w < \frac{c}{d}$, the network is in a bad environment. From the mining pool profits in Section 3.2 and Table 5, mining pool A and pool B still choose the honest mining strategy to obtain the best profit. It means that the mining pools will choose the same (H, H) strategy for p_2 as in the first stage SPE method in the infinite repeated games. After that, the optimal return R_B in a bad network can be computed by calculating the sum of the returns each time. Then, we calculate R_B by introducing the discount factor of repeated games [39]. We set δ as the discount factor. Then, according to the method of solving the sum of the returns in repeated games [38,39], we need to sum the returns of each phase of the game to obtain the total return R_B. The specific calculation performed and the results obtained are described in Equation (6).

$$\begin{aligned} R_B &= \delta * R + \delta^2 * R + \delta^3 * R + \cdots \\ &= \sum_{n=1}^{\infty} \delta^n * R \\ &= \frac{R}{1-\delta} \end{aligned} \tag{6}$$

It can be seen from Equation (6) that the benefit of the DDoS attack on the mining pool in the harsh network environment is $\frac{R}{1-\delta}$ by solving the sum of the benefits and the sum of the geometric series by infinite repeated games. Furthermore, the sum of Equation (6) consists of payoffs from honest mining in various repeated games of the pool. Thus, the total return of all subgames is the optimal return in a bad network environment with infinite game repetitions.

(2). The optimal strategy p_2 of mining pools is (D, D) when the range of values of the network environment coefficient w is $\frac{a+c}{d} < w \leq 1$. In a favorable network environment, mining pools A and B opt to initiate DDoS attacks against each other for maximum profit, similar to the scenario in the first stage of the SPE subgame outlined in Section 3.2. Then, mining pool A and mining pool B can earn the most revenue by launching DDoS attacks against each other. This revenue, referred to as R_G, can be obtained using the geometric series summation formula and the infinite repeated game payoff summation method [38,39]. Equation (7) describes the calculation and results of R_G.

$$\begin{aligned} R_G &= \delta * (R - c) + \delta^2 * (R - c) + \delta^3 * (R - c) + \cdots \\ &= \sum_{n=1}^{\infty} \delta^n * (R - c) \\ &= \frac{R - c}{1 - \delta} \end{aligned} \tag{7}$$

According to Equation (7), we can determine that the best revenue for mining pool A and mining pool B is $\frac{R-c}{1-\delta}$ after an endless game iteration in good network environments.

(3). When $\frac{c}{d} < w < \frac{a+c}{d}$, the optimal strategy p_2 in the second stage of the infinite repetition game is identical to that of pool A and pool B in the SPE method during the first stage. In a medium-scale network environment, mining pools A and B will employ a mixed strategy of honest mining and DDoS attack methods to maximize mining revenue. Also, we can gather from Section 3.2 that mining pool A and mining pool B have determined the most favorable honest mining probability by utilizing the mixed strategy probability mining of $R_M = \frac{c+a-wd}{a}$ for maximum returns. Using the probability p_1, we can determine the R_M value in infinite repeated games. The value of R_M appears in Equation (8).

$$
\begin{aligned}
R_M = {} & \delta * [\frac{-(a+c-wd)^2+(c+a)*(a+c-wd)}{a} + R - c] + \\
& \delta^2 * [\frac{-(a+c-wd)^2+(c+a)*(a+c-wd)}{a} + R - c] + \\
& \delta^3 * [\frac{-(a+c-wd)^2+(c+a)*(a+c-wd)}{a} + R - c] + \cdots \\
= {} & \sum_{n=1}^{\infty} \delta^n * [\frac{-(a+c-wd)^2+(c+a)*(a+c-wd)}{a} + R - c] \\
= {} & \frac{\frac{-(a+c-wd)^2+(c+a)*(a+c-wd)}{a} + R - c}{1-\delta} \\
= {} & \frac{-(a+c-wd)^2+(c+a)*(a+c-wd)+a*(R-c)}{a*(1-\delta)}
\end{aligned}
\tag{8}
$$

From Equation (8), we can determine that in a medium network environment, mining pool A and mining pool B will achieve optimal revenue R_M by employing a mixed strategy with an honest mining probability of $p_1 = \frac{a+c-wd}{a}$. Each term of the summation of Equation (8) is a different value of the payoff in the case of different repetitions of the game. In Equation (8), the delta represents the discount factor, which increases in each round following a first-order parametric progression. In a moderate network environment, the mining pool's payoff is represented by a complex equation, which is the sum of each term to the right. To clarify, Equation (5) is inserted into Equation (8) so that the summation represents a finite number of games. That is, different discount factors multiplied by the optimal return of a medium network for a finite number of games equals the return of a mining pool for an infinite number of repeated games.

After obtaining the optimal strategy, revenue, and mixed mining probability of a mining pool to resist DDoS attacks in three network environments, the above calculation process must be implemented via algorithms. We use Algorithm 2 to implement the TSRG approach for addressing shifts in strategy, revenue, and mining probability of mining pool A and mining pool B to resist DDoS attacks in infinitely repeated games. Algorithm 2, which solves the optimal revenue for DDoS mining pools, will be referred to as the TSRG algorithm.

The pseudo-code of Algorithm 2 elucidates how a mining pool strategy and mining income alter upon DDoS attacks in infinite repeated games. The input parameters for algorithm 2 comprise unaltered values for R, d, a, and c. Algorithm 2 results demonstrate the optimal mining strategies for pool A and pool B: $strategy_A(j,i)$, $strategy_B(j,i)$. In addition, the outputs reveal the optimal mining payoff for pool A ($payoff_A(j,i)$) and pool B ($payoff_B(j,i)$), as well as the probability of the mixed strategy ($p_A(j,i)$, $p_B(j,i)$). Line 1 of the pseudo-code initializes several parameters, including the network environment factor w, and the discount factor δ. Lines 2 to 7 indicate that the best mining approach for mining pools A and B is honest mining in a challenging network environment ($w(i) < \frac{c}{d}$). The digit "1" refers to an honest mining strategy. We determine the optimal mining return for both $payoff_A(j,i)$ and $payoff_B(j,i)$ in a bad network scenario. Pseudo-code lines 8 through 12 outline the ideal approach that mining pools A and B choose when operating in a favorable network environment ($w(i) > \frac{c+a}{d}$), which entails launching DDoS attacks against each other. The digit "2" refers to a DDoS attack strategy. Also, we can obtain the optimal mining return for both $payoff_A(j,i)$ and $payoff_B(j,i)$ in a good network environment. Lines 13–21 outline the mining pool's selection of a mixed strategy for achieving optimal returns in a medium network environment. Moreover, we can obtain the optimal mining probabilities $p_A(i)$ and $p_B(i)$ for both pools A and B, as well as the corresponding payoffs $payoff_A(j,i)$ and $payoff_B(j,i)$, which are found in this part of the pseudo-code.

Algorithm 2 A Two-Stage Repeated Game Approach to Solving Optimal Revenue Algorithms for DDoS Mining Pools

Input: R, c, d, a
Output: $strategy_A(j,i)$, $strategy_B(j,i)$. $payoff_A(j,i)$, $payoff_B(j,i)$, $p_A(i)$, $p_B(i)$.

Compute the value of w and δ
for $i \leftarrow 1$ to length(w) **do**
  for $j \leftarrow 1$ to length(δ) **do**
    if $w(i) < \frac{c}{d}$ **then**
      $strategy_A(j,i) \leftarrow 1$
      $strategy_B(j,i) \leftarrow 1$
      $payoff_A(j,i) \leftarrow \frac{R}{1-\delta(j)}$
      $payoff_B(j,i) \leftarrow \frac{R}{1-\delta(j)}$
    else if $w(i) > \frac{c+a}{d}$ **then**
      $strategy_A(j,i) \leftarrow 2$
      $strategy_B(j,i) \leftarrow 2$
      $payoff_A(j,i) \leftarrow \frac{R-c}{1-\delta(j)}$
      $payoff_B(j,i) \leftarrow \frac{R-c}{1-\delta(j)}$
    else
      $strategy_A(j,i) \leftarrow 3$
      $strategy_B(j,i) \leftarrow 3$
      $payoff_A(j,i) \leftarrow \frac{-(a+c-w(i)*d)^2+(c+a)*(a+c-w(i)*d)+a*(R-c)}{a*(1-\delta(j))}$
      $payoff_B(j,i) \leftarrow \frac{-(a+c-w(i)*d)^2+(c+a)*(a+c-w(i)*d)+a*(R-c)}{a*(1-\delta(j))}$
      $p_A(i) \leftarrow \frac{c+a-(w(i)*d)}{a}$
      $p_B(i) \leftarrow \frac{c+a-(w(i)*d)}{a}$
    end if
  end for
end for

4. Experiment and Results

After completing the theoretical analysis and solution of the repeated game method, we must compare and verify the validity and accuracy of the finite and infinite repeated game methods outlined in this paper through experimental methods. The whole experiment is divided into three parts: the evolutionary game experiment, the repeated game experiment, and the Analysis of Variance (ANOVA) experiment. The main purpose of this experiment is to validate the trends of mining pool strategies, gains, and mixing probabilities of SPE and TSRG methods. We briefly describe the experiments in this section below. First, we conduct experiments using evolutionary games to observe the trend in ideal defense strategies against DDoS attacks in mining pools with varying initial probability values. Second, we implement the SPE method in the case of finite repeated games to complete the optimal strategy, revenue, and mixed strategy changes of mining pools under DDoS attacks in different network environments. Third, we realized the TSRG method under infinite repeated game experiments to effectively make the mining pool obtain better mining income under different networks. In these experiments, the role of evolutionary games is to conduct comparative experiments with repeated games. Repeated game experiments are to verify the correctness of the results of the SPE and TSRG methods. Also, repeated game experiments realize the change in strategy and income of finite and infinite game pools. Finally, the ANOVA experiment tests the validity of mining pool returns variation with different discount factors under infinite repeated games through error analysis and hypothesis testing.

Our experiments are conducted using Matlab software on a laptop computer with Windows 11 and 16 GB of RAM. In our experiment, we simulated the situation where two mining pools in the blockchain network suffered from the revenue reduction of DDoS

attacks. The specific settings of our experimental parameters are described in Table 6. From Table 6, we can obtain that the global parameters are the honest mining revenue R, the penalty c, the reward a, and the DDoS attack revenue d under an ideal network environment ($w = 1$). Then, we set specific global parameters to values $R = 200$, $d = 60$, $a = 30$, and $c = 20$. Also, we set the value range of w in three different network environments. We also set the value of the TSRG method to a based on the change in discount factor δ. Additionally, we set x^* as the evolutionary experiment's optimal strategy and p_2 as the repeated game's strategy value. Finally, three sets of mining pool return data with delta values of 0.1, 0.4, and 0.8 were chosen for ANOVA experiments to determine if the variance of the returns is distributed according to the equilibrium of each set.

4.1. Evolutionary Game Experiment

This section presents an experiment that uses an evolutionary game to establish a mining pool that can resist DDoS attacks. Our experiment on how evolution impacts games is largely informed by earlier studies [34]. The DDoS mining pool game experiment has three sub-experiments for the different network environments. We use values of w equaling 0.1, 0.4, and 0.8, respectively, based on the varying network environment. According to three different values of w, we divide the whole evolutionary game experiment into the optimal strategy evolution experiment of the mining pool under three kinds of network conditions: bad network, medium network, and good network. We define x to represent the probability of the initial honest mining of the pool, while x^* represents the optimal strategy. In the results of the experiment, the y-axis denotes mining probability x while the x-axis represents *time*.The different colored curves in the experimental plots under all three networks represent pools with different initial probabilities of honest mining. We conducted and analyzed sub-experiments in three different network scenarios.

4.1.1. Evolutionary Game Experiments in Harsh Networks

We set the value of w to 0.1 in a challenging network environment and adjusted the mining probabilities for pool A and pool B from $x = 0.1$ to $x = 0.9$. The specific experiment is shown in Figure 8. The experimental results show that the mining probabilities of publishing different colors, ranging from $x = 0.1$ to $x = 0.9$, converge to $x = 1$. This occurs at about 0.8 s after several game iterations. It is clear from the experimental results that $x^* = 1$ is obtained after many game iterations. Thus, mining pool A and mining pool B can obtain the best returns by choosing an honest mining strategy when encountering a DDoS attack in a bad network environment. Therefore, (H, H) is the optimal mining pool strategy in a harsh network environment.

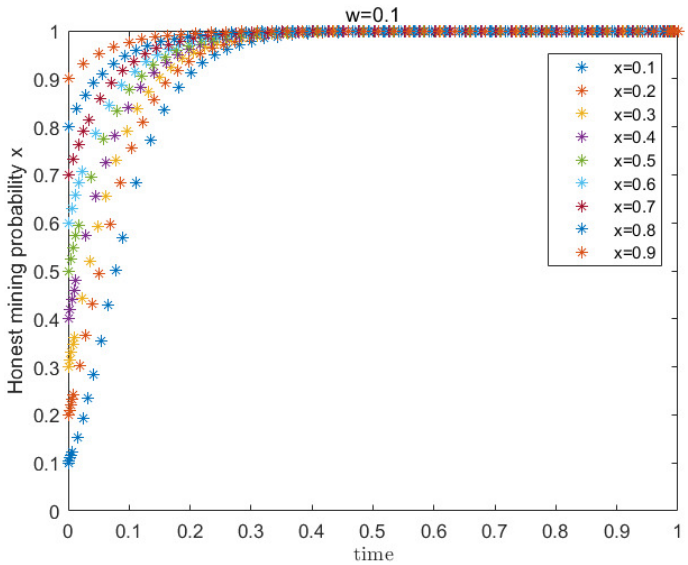

Figure 8. Evolutionary game experiment of mining pool against DDoS attack when $w = 0.1$.

The main reason why mining pools choose honest mining to obtain the best returns in harsh environments is that the uncertain network environment makes mining pools obtain fewer returns from DDoS attacks. The attack revenue wd obtained from the attack launched by the mining pool is proportional to the network environment coefficient w. The parameter w has a relatively small value in a poor network environment, consequently, wd values in DDoS attacks are also minimized. The returns of mining pools that launch DDoS attacks through the network are not as high as those of honest mining. Therefore, all mining pools with different probabilities will choose honest mining with the best returns after multiple iterations of the evolutionary game. Through this vicious network evolution game experiment, we obtain the optimal strategy of the mining pool to resist DDoS attacks $x^* = 1$. However, we cannot decide whether the number of iterations of the game is finite or infinite. Also, we cannot obtain the trend of the optimal strategy changing with the network environment coefficient w under finite and infinite games. We also cannot obtain the specific value of the optimal return of the mining pool under different game times and the trend of the change in the return with the change in the network environment. Therefore, we need to re-experiment using SPE and TSRG to solve the problems arising from the evolutionary game experiments.

4.1.2. Evolutionary Game Experiments in Medium Networks

We set the value of w to 0.4 in a challenging network environment and adjusted the mining probabilities for pool A and pool B from $x = 0.1$ to $x = 0.9$. The specific experiment is shown in Figure 9. From the experimental results, we can see that when $w = 0.4$, the mining pools, with varying probabilities, achieve $x = 0.75$ approximately 0.95 s after several game iterations. It is evident from the experimental findings that $x^* = 0.75$ is achieved after numerous game iterations. This indicates that pool A and pool B will choose the mixed strategy with honest mining probability $x^* = \frac{13}{15}$ to obtain the best returns in a medium network environment. Therefore, in the event of DDoS attacks, both mining pool A and mining pool B will implement multiple strategies to optimize their mining returns.

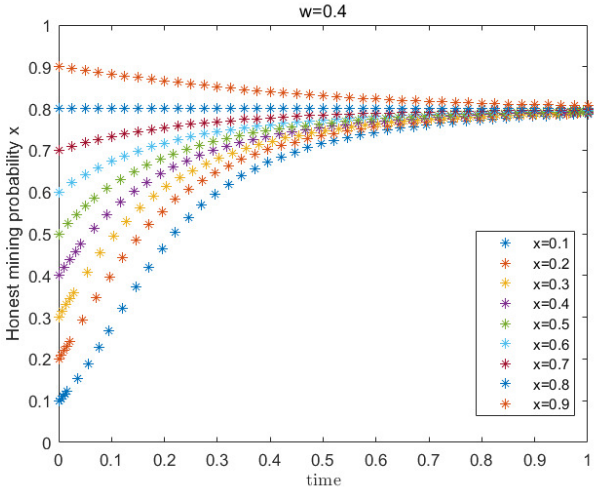

Figure 9. Evolutionary game experiment of mining pool against DDoS attack when $w = 0.4$.

The mining pool uses multiple mining methods because it can make a higher profit by launching DDoS attacks when the network environment is better. As the network environment improves, some mining pools with a lower probability of honest mining tend to launch DDoS attacks to obtain better returns, while some mining pools with a higher probability of honest mining still tend to mine honestly. This leads the mining pool to choose various mining strategies at once during multiple game iterations. The mixed mining probability is almost 0.86 in this experiment because the parameter setting calculates the mixed mining probability as $x^* = \frac{c+a-wd}{a} = \frac{13}{15}$. The evolutionary game experiment in this section can successfully determine the optimal strategy of the mining

pool. However, there are still some problems with this experiment in a medium network environment. First, the evolutionary game experiment cannot obtain the evolutionary trend of the mixed mining probability p_1 changing with w of mining pools. Second, we cannot obtain the different values and trends of optimal returns for mining pool A and mining pool B with the change in the network environment w. Therefore, it is necessary to solve these problems in a series of game experiments.

4.1.3. Evolutionary Game Experiments in Good Networks

In this section, we need to complete the DDoS attack experiment in a good network environment. We set $w = 0.8$ and the initial mining probability of the pool with nine different colors from $x = 0.1$ to $x = 0.9$. The experimental results are shown in Figure 10. From Figure 10, we can see that when the time is about 0.5 s, the mining strategy of all pools converges to $x^* = 0$. The experimental results indicate that in a good network environment, mining pools will choose to launch DDoS attacks against each other to obtain the best returns. Experimental results also show that in this case, the optimal strategy for pool A and pool B is (D, D).

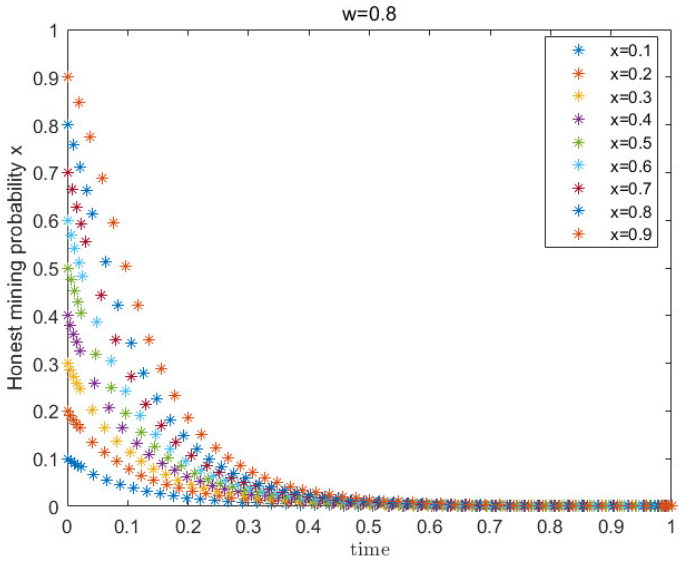

Figure 10. Evolutionary game experiment of mining pool against DDoS attack when $w = 0.8$.

The reason why mining pools choose to launch DDoS attacks in a good network environment is that the network environment is further improved based on the medium network environment, and mining pools can make more profits by launching DDoS attacks through the network. As the network situation improves, mining pools are gradually obtaining better returns by launching DDoS attacks in near-ideal network environments than by simply mining honestly. Therefore, the optimal strategy obtained by experimenting with evolutionary games in a good network environment is $x^* = 0$. Although the evolutionary game experiment can find out the optimal strategy of the mining pool, it cannot accurately reflect and obtain the optimal income of the mining pool. The evolutionary game experiment also fails to realize the changing trend of mining pool income with the network environment under the condition of finite and infinite games. Therefore, we need to solve these problems in the next repeated game experiment.

4.2. Repeated Game Experiments

After completing the evolutionary game experiment, we conduct repeated game experiments in this section to obtain the specific values and changing trends of mining strategy, optimal returns, and mixed strategy probabilities. Our repeated game experiment is divided into two parts: The SPE finite-order game experiment and the TSRG infinite-order game experiment. The SPE experiment is mainly to verify the trend of the optimal

strategy, return, and mixed strategy probability with the value of w in different network environments. The TSRG experiment is to verify and obtain the returns of mining pools under three network environments under infinite repeated games, the trend of strategy, and mining probability changing with discount factor δ. Our specific parameter settings are shown in Table 6. Also, we obtain the discounting factor δ to be $0 \leq \delta \leq 100$. The following is a description of specific experiments.

Table 6. Comparison table of specific parameters and values corresponding to the evolutionary and repeated game experiments.

One Pool Honest Mining Profit R	Illegal Profits of a Pool Launching DDoS Attacks d	Degree of Punishment or Reward by the Pool Manager a	Network Environment Coefficient w	Discount Factor δ	Analysis
$R = 60$	$d = 45$	$a = 6$	$0 \leq w < \frac{c}{d}$	$0 \leq \delta \leq 100$	Evolutionary mining strategy of the game $x^* = 1$ and repeated mining strategy of the game mining pool $p_2 = 1$.
$R = 60$	$d = 45$	$a = 6$	$\frac{c}{d} < w < \frac{c+a}{d}$	$0 \leq \delta \leq 100$	Evolutionary mining strategy of the game $x^* = \frac{13}{15}$ and repeated mining strategy of the game mining pool $p_2 = 3$
$R = 60$	$d = 45$	$a = 6$	$\frac{c+a}{d} < w \leq 1$	$0 \leq \delta \leq 100$	Evolutionary mining strategy of the game $x^* = \frac{a+c-wd}{a}$ and repeated mining strategy of the game mining pool $p_2 = 2$

4.2.1. SPE Experiments for Solving Finite Repeated Games

In this section, we conduct three sub-experiments to realize the changes in mining pool strategy, revenue, and mixed mining probability obtained by the SPE method. The mining pool policy change sub-experiment illustrates the impact of changes in the network environment on the optimal mining strategy for mining pools experiencing DDoS attacks. The experiment on mining income demonstrates how modifying the network environment coefficient w impacts the mining pool's maximum earnings. The mixed strategy change experiment is mainly to solve the influence of the network environment change on the mining probability of the mixed strategy choice.

We implement the policy change experiment when the mining pool encounters a DDoS attack according to Section 3.2 and Algorithm 1. Figure 11 shows the results of our experiment. From the experimental results, we can observe the trend of the best mining method by altering the network environment coefficient w. In the experimental results, the x-axis represents the network environment coefficient w, and the y-axis represents the mining strategy of the mining pool. The value of w ranges from 0 to 1. The mining strategy of the mining pool takes the value "1" for an honest mining strategy, "2" for the optimal profitability of launching a DDoS attack, and "3" for a mixed mining strategy. We can obtain from the experimental results that when a mining pool encounters DDoS attacks, it chooses the honest mining strategy if the network environment is relatively harsh. When the coefficient of w is between 0.3 and 0.4, which is about 0.33, the best strategy of a pool changes from an honest mining strategy to a mixed mining strategy. With the further improvement of the network environment coefficient to a good network environment, when the value of w is about 0.83, the optimal strategy changes to the optimal profit of launching DDoS attacks.

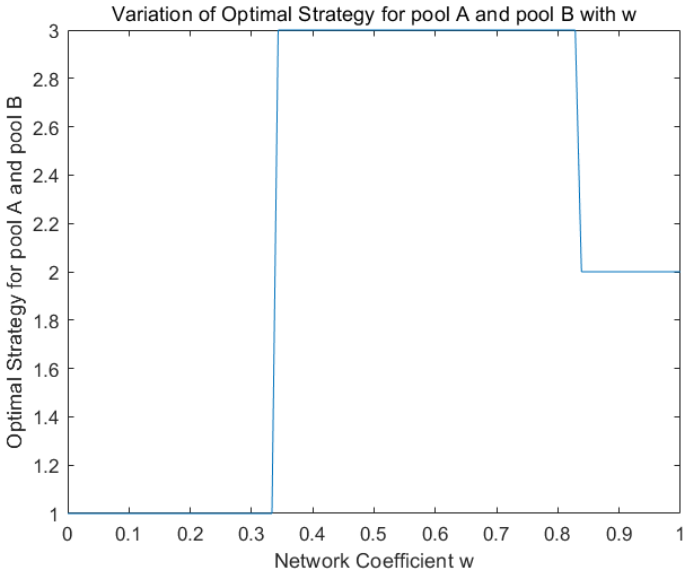

Figure 11. The changing trend of the optimal strategy of a mining pool in finite repeated games.

After completing the optimal strategy change experiment, we implement the mining pool revenue change experiment using the SPE method. The results we obtained are shown in Figure 12. As can be seen in Figure 12, the x-axis represents the network environment coefficient w, and the y-axis represents the mining income. As the network environment w changes from 0 to about 0.33, a mining pool is in a bad network environment. The payoff of the pool in this case is equal to $R_B = R = 200$. With the further improvement of the network environment, the mining pool is in the optimal profit of the mixed strategy. The payoff in this part is equal to the R_M value in Equation (5) of Section 3.2. The returns of the pool and w form a parabolic curve, and the power of w is negative. Therefore, the pool's returns first increase with w and then decrease as w increases to an extreme value. In the results of the mixed strategy experiments, the returns of the mining pool also increase with w finally reaching an extreme value at approximately equal to 0.43, and finally, gradually the returns decrease with w. This is consistent with the change in returns embodied in Equation (5). Finally, we find that the mining pool is in a good network state when w is approximately equal to 0.83. We obtain the value of the optimal return, which is equal to the value of R_G, as $R - c = 200 - 20 = 180$.

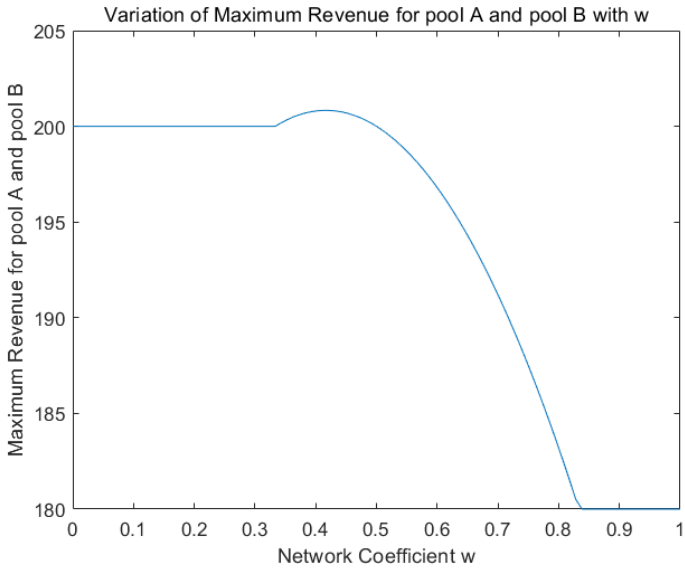

Figure 12. The changing trend of the optimal mining revenue of a mining pool in finite repeated games.

After completing the above two sub-experiments, we need to solve for the optimal honest mining probability and the trend of the mining pool's w-change in the mixed strategy. The specific experiment is shown in Figure 13. We can see from Figure 13 that the horizontal coordinate is the network environment coefficient w, and the vertical coordinate is the honest mining probability p_1. A value of 0 for p_1 indicates that the mining pool is in a single DDoS attack or an honest mining pure strategy phase. The linear inverse relationship between the mining probability of the mixed strategy and w can be obtained by changing w and Equation (3). We can see from the experimental results that the mining probability of the mining pool mixing strategy gradually decreases from 1 to 0 when w is about 0.33. There is also a linear inverse relationship between the probability of honest mining in the mining pool and the coefficient of the network environment, which is consistent with our theoretical analysis results in Section 3.2.

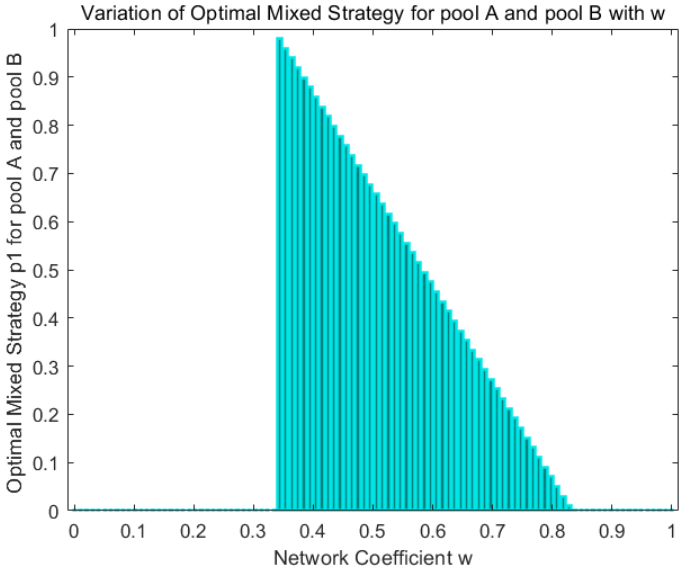

Figure 13. The changing trend of mixed mining probability of a mining pool in finite repeated games.

4.2.2. TSRG Experiments for Solving Infinite Repeated Games

After completing the SPE experiment, we complete this section by using the TSRG method to solve the optimal mining pool strategy, the change in returns, and the mixed mining probability under the infinite repetition game. Our TSRG experiments are consistent with those in Section 4.2.1 and include three parts: the optimal strategy selection, the variation of best mining revenue, and the evolution trend of the mixed strategy probability. The experiment of mining pool strategy change is mainly to realize the trend that the optimal strategy changes with the change in network environment under infinite games. The income experiment of mining pools is mainly to realize the mining income under infinite game times obtained by the TSRG method and algorithm two through the experiment. The mixed strategy mining return probability experiment is to realize the changing trend of the optimal mixed mining probability when the mining pool changes with the network environment under the infinite repeated game. The parameters in Table 6 are mainly used to set our specific experimental parameters and values. The difference from Section 4.2.1 is that we set another parameter, the discount factor δ. δ is set to the value of $0 \leq \delta \leq 100$.

After setting the parameters, we realized the experiment of the optimal strategy change for mining pools under infinitely repeated games. The specific experimental results are shown in Figure 14. We can see from the experimental results that the x-axis represents the network environment coefficient w, the y-axis represents the discount factor δ, and the z-axis represents the mining strategy. The optimal strategy of the mining pool changes only with w, not with the discount factor δ. Therefore, the result of optimal strategy selection in the infinite repeated game mining pool is the same as the result of the SPE strategy change experiment in Section 4.2.1 above. The network environment is in a bad state when

w increases from 0 to nearly 0.33. In this case, pool A and pool B choose the best honest mining strategy. When the value of w changes from about 0.33 to about 0.83, the mining pools in a medium network condition all choose the mixed mining strategy to make the best profit. When w changes from about 0.83 to 1, mining pools decide to launch DDoS attacks against each other in a good network environment to obtain the best returns. The selection of the optimal strategy of the infinite repeated game mining pool is consistent with the results of the evolutionary game experiment in Section 4.1 and the SPE experiment in Section 4.2.1. At the same time, the experimental results in this section are consistent with the theoretical results of the TSRG method in Section 3.3. This shows the correctness of our method and experiment.

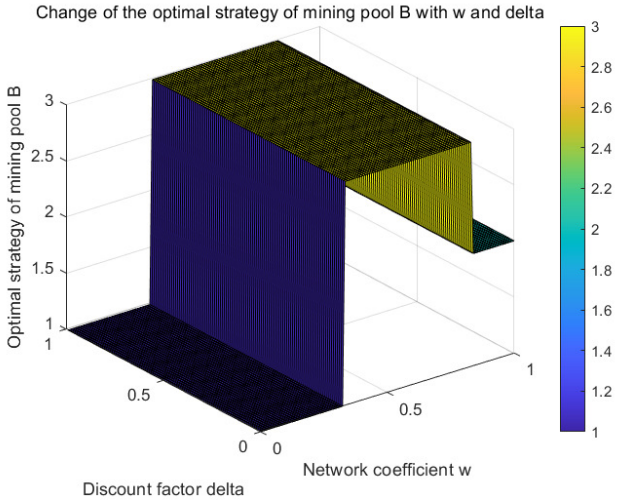

Figure 14. The changing trend of the optimal strategy of a mining pool in infinite repeated games.

The experimental results of the probability change for the mixed strategy under the TSGR method are shown in Figure 15. We can see from the experimental results that the mixed strategy change in the TSRG method in this paper is independent of the value of the discount factor δ. Only the network environment coefficient w affects the mixed mining probability p_1. In the experimental results, the X-axis represents w, the Y-axis represents δ, and the Z-axis represents the p_1 mining probability of the mixed strategy. When p_1 equals 0, it is the case of a single honest mining or DDoS attack pure strategy, not the case of a mixed strategy with multiple mining strategies. We can obtain that the change in p_1 follows Equation (3). The mixed mining probability p_1 decreases inversely with the increase in the network environment coefficient w. This indicates that the honest mining probability of the mining pool decreases with the improvement in the network environment in the medium network environment. Therefore, mining pools gradually have a higher probability of using mixed strategies to select DDoS attacks for optimal returns.

The mining profit experiment in infinite repeated game times is an experiment to realize the change in optimal profit for a mining pool with the network environment by the TSRG method. Our experimental results are shown in Figure 16. From Figure 16, we can see that the X-axis represents the network environment coefficient w, the Y-axis represents the discount factor δ, and the Z-axis represents the optimal returns under different network environments. The different colored curves in Figure 16 represent the values of the mining pool returns, which are constantly changing with the discount δ. If the value of the discount factor δ is unchanged, we can see that the revenue of the mining pool first tends to stabilize with the increase in the network environment coefficient w. When w is approximately 0.33, the revenue of the mining pool first increases and then decreases. Finally, when w is about 0.83, the revenue of the mining pool drops to the lowest value and does not change. If w is constant, the discount factor δ increases and the income of the mining pool gradually increases. The reasons for this experimental result are as follows: First, as w changes from 0 to about 0.33, the mining pool is in a bad network environment. The change in the

value of the pool returns follows the value of R_B in Equation (6). The optimal profit of the mining pool remains equal to the value of R_B without changing. When w is approximately between 0.33 and 0.83, the mining pool is in a medium network environment. The optimal revenue of the mining pool follows Equation (8). We can see through Equation (8) that δ is constant with the optimal return of the mining pool alongside w into a quadratic equation relationship. The optimal revenue of the mining pool first increases to a maximum value with the increase in the network environment w, and then gradually decreases from the maximum value. When w changes from about 0.83 to 1, the mining pool is in a good network condition. The returns of the mining pool in this case follow Equation (7). The optimal gain for the mining pools in this case is consistent with the gain from launching DDoS attacks against each other, which is less than the gain in any other case. Second, from Equations (6)–(8) we can obtain that the value of the discount factor δ is proportional to the mining revenue. The higher the discount factor δ, the higher the mining revenue. The discount factor δ mainly refers to the fact that we are extrapolating future returns to present returns. Thus, the higher the discount factor, the more future returns we obtain when calculating the optimal returns we obtain now, and the higher the returns we obtain for infinite games. Our designed TSRG method achieves the best earnings value by taking into account the discount factor delta. A lower δ value leads to less future earnings being converted to current earnings and a lower optimal earnings value.

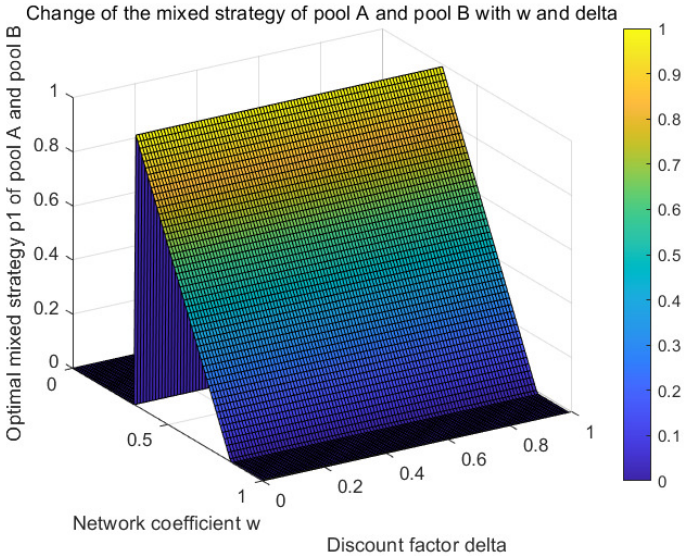

Figure 15. The changing trend of mixed mining probability of a mining pool in infinite repeated games.

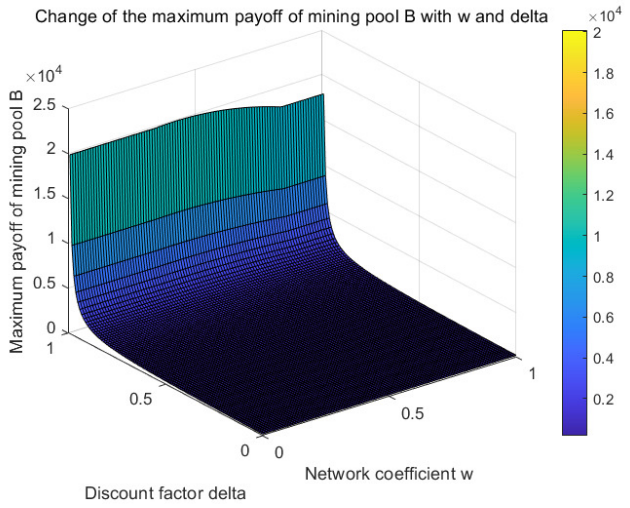

Figure 16. The changing trend of the optimal mining revenue of a mining pool in infinite repeated games.

4.3. ANOVA Experiments

The Analysis of Variance (ANOVA) experiment serves to compare whether the means of at least three sets of data are significantly different [40]. ANOVA is a hypothesis testing method that uses sample data to infer characteristics of the overall population. Specifically, it tests whether the overall means of the groups are equal or whether some groups have significantly higher or lower means than others. The null hypothesis of ANOVA is that the overall means of the groups are equal, and the alternative hypothesis is that at least two groups have unequal overall means [41].

The basic principle of ANOVA is to decompose the total variance into between-group variance and within-group variance, and then calculate the ratio of the two, known as the F-statistic [42]. A larger F-statistic indicates a greater proportion of between-group variance to the total variance, which means that the difference in means between each group is more significant. The distribution of the F-statistic depends on the degrees of freedom, which are the between-group degrees of freedom and the within-group degrees of freedom. The p-value for the F-statistic can be obtained by either looking it up in a table or calculating its probability. This value is used to determine whether to reject the null hypothesis [43]. Therefore, if the p-value is greater than the significance level, we must accept the null hypothesis. Conversely, if the p-value is less than or equal to the significance level, we reject the null hypothesis and accept the alternative hypothesis. In general, the initial value of the significance level is set at 0.05. In this paper, the mining revenue strategy is a fixed strategy value that does not participate in the error analysis. The probability value of hybrid mining is a hybrid strategy that is a decision problem which is also not involved in hypothesis suggestion [44]. The only experimental data involved in the analysis of variance in this paper are the optimal returns in different network environments.

If there are a limited number of repeated games, the mining pool's strategy, returns, and hybrid mining probabilities will closely change with the network environment. However, these data on gain values are only continuous data that change with the network environment. ANOVA analysis does not support analysis of continuous gain data, only error detection for categorical or discrete data. Meanwhile, ANOVA is typically used to compare whether sample means are significantly different across groups (e.g., different treatment conditions or different time points). The earnings data from these different network environments lack comparisons of sample means across multiple groups, so ANOVA may not be applicable here.

In an infinitely repeated game environment, the returns of the mining pool change as the network environment and the discount factor interact. In the same network environment, there are infinite simultaneous observations of the optimal returns of the mining pools as the discount factor delta varies. Thus, it is possible to conduct hypothesis testing and error analysis on the optimal returns of mining pools in all network environments using the ANOVA method with varying values of the discount factor δ. The steps of our ANOVA experiment are shown in the description below.

We use it in the statistical and error tests in our ANOVA experiments to check whether there is a significant difference in the average of the optimal returns. In this particular experiment, we compute the optimal strategies and maximum returns for mining pools A and B under different network coefficients and discount factors. Then, we set three δ values of 0.1, 0.4, and 0.8. We verify the validity of the results of our repeated game experiments by analyzing the errors of these three sets of data through ANOVA experiments. Additionally, it is assumed that the mean data are approximately equal across all three data sets. Alternatively, the error in the mean values of the three data sets may be too large.

The ANOVA test results are presented, including the F-statistic and p-value, which can determine if there is a significant difference in means between groups. Our experimental results yield a p-value greater than 0.05, indicating that the model in this paper concludes there is no significant difference in the experimental results. Thus, the RGD method presented in this paper satisfies the ANOVA test and the experimental outcomes are valid.

The results of our experiments are shown in Table 7. The table's SS, df, MS, and F values have little effect on the experimental results and are only used in variance calculations. We will not analyze their significance. Instead, we will focus on the experimental results p-value. The experiment's p-value is 0.9461, which is greater than our design's significance level of 0.05. This indicates that the original hypothesis, which states that the mean value of the returns of the three groups of mining pools is equal, is valid. Therefore, the experimental results of this paper align with the expected error.

Table 7. Results of the ANOVA experiment.

Data Sources	SS	df	MS	F	p-Value
Intergroup values	579,438.5	2	289,719.3	0.06	0.9461
Error value	1,551,846,397.8	297	5,225,072	Null	Null
Total	1,552,425,836.4	Null	Null	Null	Null

The results of the same experiment are shown in Figure 17. The experimental results show that the three data sets are evenly distributed among the different groups, as represented by the return values on the y-axis. The x-axis indicates the group number. The three groups of experiments do not affect each other's return values. The red cross line in the graph represents the return values for each group and the blue line represents the margin of error. The change in delta has an error on the optimal return of the mining pool within the effective range. Therefore, the RGD method described in this paper is effective.

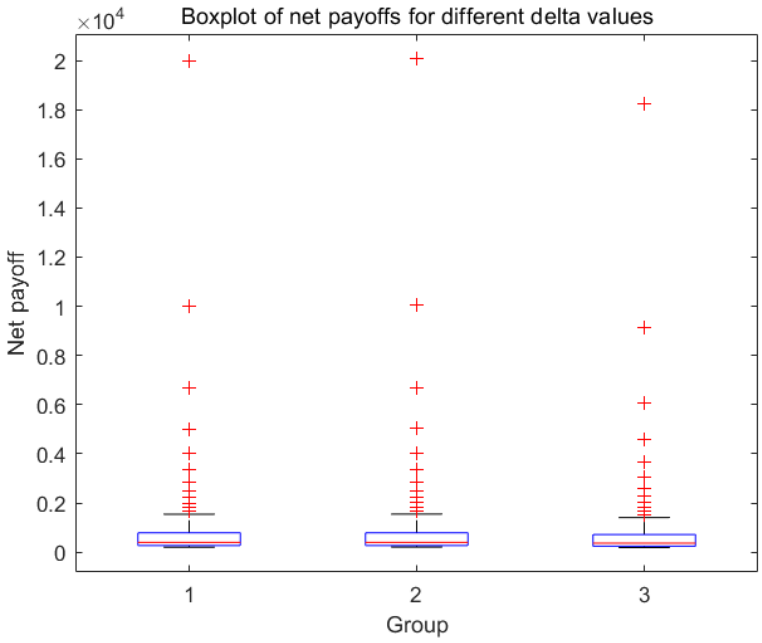

Figure 17. ANOVA experimental results.

5. Discussion

This study focuses on mining pools with the same computational power and what will be the outcome of the proposed scheme if the mining pools of different powers defend against DDoS attacks.

Optimal mining strategies for asymmetric arithmetic mining pools experiencing DDoS attacks under different network environment scenarios is a complex problem. This problem differs from the symmetric arithmetic case discussed in this paper and requires more sophisticated modeling and solution methods for implementation. The specific work is very complex and tedious, and we plan to complete and implement this work in the future. Our plans are roughly as follows:

(1). The asymmetric model requires the creation of replica dynamical systems that are more complex than the current model to determine stable solutions in a more detailed network environment. The optimal mining strategy for different networks with different arithmetic powers is then obtained according to the Friedman method.

(2). Next, in the finite repetition game, we plan to calculate the revenue matrix of each mining pool based on the arithmetic ratio of the two pools, and then divide it into three scenarios based on the difference in network environment coefficients w, and solve the optimal strategy and revenue in each scenario separately.

(3). Finally, in the infinite game case, we plan to use the TSRG method to take the subgame of the first stage as the result of the SPE strategy, and the repeated game of the second stage as an infinite number of iterations, to introduce a global discount factor δ, to compute the expected return of each mining pool based on the arithmetic ratio of the two pools, and then to divide three cases according to the difference in the network environment coefficients w, and to solve the optimal strategy and return for each case separately.

6. Conclusions and Future Works

In this paper, we propose a mitigation method for DDoS attacks on mining pools based on the repeated game method. To counter DDoS attacks, the implementation of this method can effectively alleviate the problem of mining pools in various networks. Also, we use the SPE method to solve the optimal strategy, revenue, and mixing probability of a mining pool under a DDoS attack in the finite repeated game environment. Finally, we implemented the TSRG method to obtain the changing trend of mining strategy and mining pool revenue against DDoS attacks in different network environments. The comparison results indicate that repeated game experiments can address the disadvantage of evolutionary game experiments in achieving optimal returns for mining pools and adapting mixed strategies to DDoS attacks on the network. The experiments on finite and infinite repetition games demonstrate that as the network coefficients increase, the optimal strategies and returns of mining pools tend to decrease. Mixed-strategy experiments illustrate that the mixed mining probability first increases and then decreases as the network environment factor increases. At the same time, the infinite repetition of the game experiment also shows the trend of decreasing returns of the mining pool with the increase in the discount factor. ANOVA experiments demonstrate the correctness and effectiveness of our designed RGD method. However, there are many areas for improvement in the current work of this paper. First, the SPE and TSRG methods we developed are appropriate for two mining pools with equal computational power. Therefore, in the future, we will improve the current RGD approach by mining pools with different computing power to defend against DDoS attacks. Second, the designed RGD approach is proposed to simulate a virtual environment. Thus, we will enhance the model from this paper to satisfy the security requirements of systems and meet the security needs of applications in reality.

Author Contributions: Conceptualization, Q.W. and Z.H.; methodology, Z.H. and X.L.; software, Z.H. and X.L.; validation, Z.H., Y.C. (Yin Chen), Y.C. (Yuan Cao) and X.L.; writing—original draft preparation, X.L. and Z.H.; writing—review and editing, Z.H., Y.C. (Yin Chen) and Q.W.; supervision, Z.H. and Q.W.; project administration, Z.H., Y.C. (Yin Chen), Q.W. and Y.C. (Yuan Cao); funding acquisition, Q.W., Y.C. (Yuan Cao) 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 Guangzhou Municipal Science and Technology Project under grant SL2022A04J00404, 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, and in part by the Key Laboratory of Smart Human Computer Interaction and Wearable Technology of Shaanxi Province.

Data Availability Statement: Data are contained within the 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 conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PoW	Proof of Work
BWH	Block Withholding Attacks
SM	Selfish Mining
DDoS	Distributed Denial of Service
BDoS	Incentive-Based Denial of Service
IoT	Internet of Things
RGD	Repeated Game-Based DDoS Attack Mitigation
TSRG	Two-Stage Repeated Game
SPE	Subgame Perfect Equilibrium
ANOVA	Analysis of Variance

References

1. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, D. Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *3*, 1977–2008. [CrossRef]
2. Duan, L.; Sun, Y.; Ni, W.; Ding, W.; Liu, J.; Wang, W. Attacks Against Cross-Chain Systems and Defense Approaches: A Contemporary Survey. *IEEE/CAA J. Autom. Sin.* **2023**, *8*, 1647–1667. [CrossRef]
3. 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**, *4*, 2604. [CrossRef]
4. Zhou, C.; Xing, L.; Liu, Q.; Wang, H. Effective Selfish Mining Defense Strategies to Improve Bitcoin Dependability. *Appl. Sci.* **2023**, *13*, 422. [CrossRef]
5. Zhang, Y.; Chen, Y.; Miao, K.; Ren, T.; Yang, C.; Han, M. A Novel Data-Driven Evaluation Framework for Fork after Withholding Attack in Blockchain Systems. *Sensors* **2022**, *22*, 9125. [CrossRef] [PubMed]
6. Li, Y.; Wang, J.; Zhang, H. A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces. *J. Netw. Comput. Appl.* **2023**, *217*, 103686. [CrossRef]
7. 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**, *8*, 4953. [CrossRef]
8. Chaganti, R.; Bhushan, B.; Ravi, V. A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. *Comput. Commun.* **2023**, *197*, 96–112. [CrossRef]
9. Ibrahim, R.F.; Abu Al-Haija, Q.; Ahmad, A. DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors* **2022**, *18*, 6806. [CrossRef]
10. Du, M.; Wang, K.; Liu, Y.; Qian, K.; Sun, Y.; Xu, W.; Guo, S. Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security. *IEEE Wirel. Commun.* **2020**, *3*, 38–45. [CrossRef]
11. Wani, S.; Imthiyas, M.; Almohamedh, H.; Alhamed, K.M.; Almotairi, S.; Gulzar, Y. Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry* **2021**, *2*, 227. [CrossRef]
12. Liu, Z.; Luong, N.C.; Wang, W.; Niyato, D.; Wang, P.; Liang, Y.-C.; Kim, D.I. A Survey on Applications of Game Theory in Blockchain. *arXiv* **2019**, arXiv:1902.10865.
13. Rodrigues, B.; Scheid, E.; Killer, C.; Franco, M.; Stiller, B. Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks. *J. Netw. Syst. Manag.* **2020**, *4*, 953–989. [CrossRef]
14. Wang, H.; An, J. Dynamic stochastic game-based security of edge computing based on blockchain. *J. Supercomput.* **2023**, *14*, 15894–15926. [CrossRef]
15. 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]
16. Elubeyd, H.; Yiltas-Kaplan, D. Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined Networks. *Appl. Sci.* **2023**, *13*, 3828. [CrossRef]
17. Ma, R.; Wang, Q.; Bu, X.; Chen, X. Real-Time Detection of DDoS Attacks Based on Random Forest in SDN. *Appl. Sci.* **2023**, *13*, 7872. [CrossRef]

18. Platt, M.; McBurney, P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* **2023**, *16*, 34. [CrossRef]
19. Wenhua, Z.; Qamar, F.; Abdali, T.-A.N.; Hassan, R.; Jafri, S.T.A.; Nguyen, Q.N. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics* **2023**, *3*, 546. [CrossRef]
20. Cai, T.; Jia, T.; Adepu, S.; Li, Y.; Yang, Z. ADAM: An Adaptive DDoS Attack Mitigation Scheme in Software-Defined Cyber-Physical System. *IEEE Trans. Ind. Inform.* **2023**, *6*, 7802–7813. [CrossRef]
21. Rajan, D.M.; Sathya Priya, S. DDoS mitigation techniques in IoT: A Survey. In Proceedings of the 2022 International Conference on IoT and Blockchain Technology (ICIBT), Ranchi, India, 6–8 May 2022; pp. 1–7. [CrossRef]
22. Mishra, S. Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy. *Electronics* **2023**, *16*, 3524. [CrossRef]
23. Truong, V.; Le, L.B. MetaCIDS: A Metaverse Collaborative Intrusion Detection System based on Blockchain and Federated Learning. *Techrxiv Prepr*. **2023**, *2*, 1–7. [CrossRef]
24. Su, J.; Jiang, M. A Hybrid Entropy and Blockchain Approach for Network Security Defense in SDN-Based IIoT. *Chin. J. Electron*. **2023**, *3*, 531–541. [CrossRef]
25. 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**, *4*, e4729. [CrossRef]
26. Johnson, B.; Laszka, A.; Grossklags, J.; Vasek, M.; Moore, T. Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools. In *Proceedings of the Financial Cryptography and Data Security, Christ Church, Barbados, 7 March 2014*; Böhme, R., Brenner, M., Moore, T., Smith, M., Eds.; Springer: Berlin/Heidelberg, Germany; Volume 8438, pp. 72–86. [CrossRef]
27. 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]
28. Alzahrani, N.; Bulusu, N. Towards True Decentralization: A Blockchain Consensus Protocol Based on Game Theory and Randomness. In *Proceedings of the Decision and Game Theory for Security: 9th International Conference (GameSec 2018), Seattle, WA, USA, 29–31 October 2018*; Bushnell, L., Poovendran, R., Başar, T., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 465–485. [CrossRef]
29. Kaci, A.; Rachedi, A. PoolCoin: Toward a distributed trust model for miners' reputation management in blockchain. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6. [CrossRef]
30. 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. [CrossRef]
31. 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 (CCS), Virtual Event, 9–13 November 2020; pp. 601–619. [CrossRef]
32. 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**, *2*, 874–887. [CrossRef]
33. Sharma, D.D.; Lin, J.; Sarojwal, A.; Sharma, A.; Sharma, A. Blockchain-Based Adaptive Non-Cooperative Game Strategy For Smart Power Contracts. In Proceedings of the 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, 7–9 April 2023; pp. 1–6. [CrossRef]
34. Liu, X.; Huang, Z.; Wang, Q. Evolutionary Equilibrium of Mining Pools Under DDoS Attack in Blockchain System. In Proceedings of the 2023 International Conference on Networking and Network Applications (NaNA), Qingdao, China, 18–21 August 2023; pp. 78–83. [CrossRef]
35. Riedel, F.; Steg, J.-H. Subgame-perfect equilibria in stochastic timing games. *J. Math. Econ*. **2017**, *72*, 36–50. [CrossRef]
36. Mastrogiacomo, E.; Tarsia, M. Subgame-perfect equilibrium strategies for time-inconsistent recursive stochastic control problems. *J. Math. Anal. Appl.* **2017**, *2*, 127425. [CrossRef]
37. Kim, J. The effects of time preferences on cooperation: Experimental evidence from infinitely repeated games. *Am. Econ. J. Microeconomics* **2023**, *1*, 618–637. [CrossRef]
38. Mertens, J.-F. Repeated games. In *Game Theory and Applications*; Academic Press: Cambridge, MA, USA, 1990; pp. 77–130. [CrossRef]
39. Fudenberg, D.; Maskin, E. The folk theorem in repeated games with discounting or with incomplete information. *Long-Run Collab.-Long-Run Games* **2009**, *2009*, 209–230. [CrossRef]
40. Wold, S. Analysis of variance (ANOVA). *Chemom. Intell. Lab. Syst.* **1989**, *4*, 259–272. [CrossRef]
41. Ermergen, T.; Taylan, F. Investigation of DOE model analyses for open atmosphere laser polishing of additively manufactured Ti-6Al-4V samples by using ANOVA. *Opt. Laser Technol*. **2024**, *168*, 109832. [CrossRef]
42. Acal, C.; Aguilera, A.M. Basis expansion approaches for functional analysis of variance with repeated measures. *Adv. Data Anal. Classif.* **2023**, *2*, 291–321. [CrossRef] [PubMed]

43. Szewczyk, M.; Szwajka, K. Assessment of the Tribological Performance of Bio-Based Lubricants Using Analysis of Variance. *Adv. Mech. Mater. Eng.* **2023**, *1*, 31–38. [CrossRef]
44. Bakht, K.; Kashif, S.A.R.; Fakhar, M.S.; Khan, I.A.; Abbas, G. Accelerated Particle Swarm Optimization Algorithms Coupled with Analysis of Variance for Intelligent Charging of Plug-in Hybrid Electric Vehicles. *Energies* **2023**, *16*, 3210. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.