

Article

Dynamic Evolutionary Game and Convergence Analysis of Mining Pool Strategies Under DDoS Attacks for IoT-Oriented Blockchain Systems

Xiaozhen Cheng ¹, Xiao Liu ^{2,*} , Zhaozhan Li ¹, Dong Ding ³ , Yuning Zhao ³, Jinping Li ⁴  and Zhixue Wang ^{5,*}

¹ College of Air and Missile Defense, Air Force Engineering University, Xi'an 710051, China; zhenxiaocheng2003@163.com (X.C.); 18191029516@189.cn (Z.L.)

² School of Computer Science, Zhongyuan University of Technology, Zhengzhou 450007, China

³ School of Computer Science and Technology, Xidian University, Xi'an 710071, China; dingdong@xidian.edu.cn (D.D.); zhaoyun@stu.xidian.edu.cn (Y.Z.)

⁴ School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an 710121, China; lijinpings@stu.xupt.edu.cn

⁵ School of Mathematics and Computer Science, Ningxia Normal University, Guyuan 756000, China

* Correspondence: cantona@zut.edu.cn (X.L.); nxwzx@nxnu.edu.cn (Z.W.); Tel.: +86-135-9207-9891 (X.L.); +86-139-9504-8069 (Z.W.)

Abstract

Distributed Denial-of-Service (DDoS) attacks are a major security threat to blockchain systems, especially in Internet-of-Things (IoT)-oriented and edge-assisted deployments where mining services, gateway nodes, and communication resources are more vulnerable to disruption. In Proof-of-Work (PoW) blockchain networks, such attacks can degrade mining pool connectivity, reduce effective revenue, and undermine both system security and resilient infrastructure design. Existing studies have mainly focused on DDoS detection or static mining games, while paying limited attention to dynamic strategy evolution and convergence under varying network conditions. To address this problem, this paper proposes a dynamic evolutionary game (DEG)-based revenue model for mining pools under DDoS attacks. Unlike static game methods that only identify equilibrium points, this work analyzes both the convergence dynamics and the sensitivity of equilibrium outcomes to key parameters, including attack scale, penalty, reward, and network quality. The proposed method characterizes the adaptive interaction between honest mining and attack behaviors through replicator dynamics, and analyzes strategy stability and convergence using equilibrium and Lyapunov-based methods. In addition, we investigate how key system parameters, including attack scale, reward, penalty, and network quality, affect the convergence speed of mining pool strategies in different environments. MATLAB results show that the proposed DEG model better captures the dynamic evolution of mining pool behaviors than conventional static-game formulations. The results further indicate that improved network conditions may unintentionally incentivize DDoS attacks, while proper parameter tuning can accelerate convergence toward security-favorable strategies. These findings provide useful insights for secure blockchain design and resilient mining infrastructure in IoT-oriented systems.

Keywords: DDoS attacks; blockchain-enabled IoT; mining pool; dynamic evolutionary games; convergence analysis; cybersecurity; resilient infrastructure



Academic Editor: Fabio Grandi

Received: 10 June 2026

Revised: 21 July 2026

Accepted: 26 July 2026

Published: 30 July 2026

Copyright: © 2026 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.

1. Introduction

Proof of Work (PoW) is one of the most commonly used consensus mechanisms in blockchain systems [1] and has been widely applied in large public chain-related scenarios, such as smart healthcare, smart homes, cloud computing, hardware security and Internet of Things (IoT) environments [2]. PoW allows mining pools to obtain rewards through computational competition. However, such fierce competition also creates opportunities for malicious mining pools to launch attacks and obtain illegal revenue. Attackers typically utilize fake virtual Internet Protocol (IP) addresses, create redundant forks, and cut off miners from mining websites to obtain the mining rewards of honest mining pools [3]. Among these attacks, Distributed Denial of Service (DDoS) attacks are one of the most frequent and harmful security threats within blockchain systems. When launching a DDoS attack, hackers send excessive network requests to a target through the blockchain network to cut it off from the mining site. Subsequently, the adversary captures the historical block rewards generated by the victim pool [4]. In blockchain-enabled IoT and edge-oriented environments, DDoS attacks reduce the payoff of honest mining as well as the right and opportunity to continue mining for more revenue [5], which ultimately decreases the overall benefits of blockchain incentives for node mining. Therefore, it is an urgent problem to mitigate revenue loss caused by DDoS attacks in PoW-based blockchain systems.

Significant studies have been conducted in recent years [6–10] to address the risks associated with DDoS attacks in blockchain networks. These studies include machine learning (ML)-based DDoS detection methods and game-based DDoS attack modeling strategies. ML-based detection methods use advanced algorithms to analyze and classify traffic data and network request volumes in blockchain networks, aiming to identify anomalous traffic and excessive requests [11–13]. While these methods can effectively defend against DDoS attacks, they require significant additional resources, which can degrade the performance of blockchain systems. In addition, ML-based methods fail to address the issue of mining revenue loss caused by DDoS attacks. In response, the DDoS static game method uses Nash equilibrium to derive optimal mining pool strategies, improving blockchain security and profitability [14–16]. However, while game methods are effective in identifying equilibrium strategies, they lack the capacity to analyze strategy evolution under changing network conditions. Static games assume pools reach equilibrium instantaneously and do not provide convergence analysis that captures how systems evolve over time. Moreover, existing game-theoretic studies predominantly focus on proving equilibrium existence rather than analyzing convergence dynamics and how key parameters affect convergence speed. These limitations obscure critical insights about mining pool adaptation and blockchain security management. To address these limitations, it is necessary to model DDoS profits using a dynamic evolutionary game approach.

Our previous work [16,17] introduced dynamic evolutionary game approaches to DDoS analysis but had three main limitations: the model was oversimplified, convergence analysis was absent, and parameter sensitivity was not thoroughly evaluated. To overcome these limitations, we now develop a more comprehensive model that integrates variable network conditions and adaptive mining pool behaviors, using replicator dynamics and Lyapunov methods to analyze strategy evolution and convergence. To enhance robustness, we conduct sensitivity analyses on key parameters, including node count and incentive mechanisms. Simulation experiment results obtained using MATLAB verify that improved network conditions incentivize DDoS attacks and that adjusting control variables can significantly accelerate strategy convergence. These findings provide insights into how economic incentives affect blockchain security. Our work goes beyond static equilibrium analysis to capture the dynamic adaptation of mining pools under changing conditions. In particular, the main contributions of this paper are as follows:

- Our work provides a dynamic evolutionary game analysis of mining pool strategy evolution under DDoS attacks and investigates convergence using replicator dynamics and Lyapunov-based stability analysis.
- We model mining pool profitability under DDoS attacks as an optimal strategy problem, solved via replicator dynamics and Lyapunov analysis across varying network conditions.
- We analyze the DDoS profit model's convergence to ensure rapid strategy optimization and minimize mining pool revenue loss under varying network conditions.
- Compared to static games, the DEG-based method better captures mining pool convergence under varying conditions, with experiments showing that parameter tuning in improved networks speeds convergence and strengthens security.

The rest of the paper is organized as follows: Section 2 outlines the background of DDoS attacks in blockchain. Section 3 presents the proposed DEG-based model. Optimal strategy solution and convergence analysis are presented in Section 4. The experimental results and analysis are presented in Section 5. Section 6 discusses the limitations of the model assumptions and relevant extensions. Conclusions and future works are provided in Section 7.

2. Related Work

2.1. DDoS Attack Detection and Mitigation Methods

To address the DDoS threat in blockchain, many researchers have proposed various methods [18–23], which include DDoS attack detection and DDoS gaming methods [24–26].

DDoS detection methods utilize machine learning (ML) algorithms to detect excessive traffic or several network requests to anticipate DDoS attacks. Yakubu et al. [27] proposed a lightweight authentication mechanism that enables safe Device-to-Device (D2D) interactions in a smart home. This method uses a single server queuing system model and the authentication mechanism to curtail DDoS attacks by controlling the number of service requests in the blockchain system. Shirvani et al. [28] proposed an improved federated learning (FL) method for IoT DDoS detection. This method addresses the privacy and efficiency limitations of traditional ML and also mitigates the resource constraints and non-IID data challenges in FL through deep autoencoders, retraining, and partial selection. Dai et al. [29] proposed a distributed DDoS-attack traffic-detection method based on a cross-multilayer convolutional neural network model in the blockchain network layer. This method effectively solves the problem that DDoS attacks using hybrid network protocols in blockchain are difficult to detect. Yazdinejad et al. [30] designed a secure, intelligent fuzzy blockchain framework to utilize a novel fuzzy deep learning model, optimized adaptive neuro-fuzzy inference system (ANFIS)-based attack detection, fuzzy matching (FM), and fuzzy control system (FCS) to defeat DDoS attacks in the block networks.

The game-theoretic approach models DDoS attacks by translating payoff outcomes into a revenue matrix, from which the mining pool's optimal strategy is obtained by solving for the Nash equilibrium. This method helps mitigate revenue loss for mining pools under DDoS attacks. Huang et al. [16] proposed a DDoS attack mitigation method based on dynamic evolutionary games. The method can solve the optimal revenue strategy for mining pools under different network environments. Wu et al. [31] implemented a DDoS attack mitigation method utilizing a stochastic game. This method can effectively solve the problem of reduced revenue from DDoS attacks when blockchain mining pools compete with each other for mining revenue. Johnson et al. [32] proposed a DDoS attack mitigation method based on static games for mining pools. This approach effectively balances these strategies with a series of game-theoretical models of competition between two pools of competition of varying sizes. Zheng et al. [33] proposed a novel game-theoretic analysis

model by adding the DDoS defense cost to defend the mining pools in the blockchain system against DDoS attacks. Sood et al. [34] proposed a static game approach to solving the miners' revenue and price mitigation model with DDoS attack costs. This model effectively alleviates the revenue loss of miners defending against DDoS attacks.

2.2. Dynamic Game Approaches to Mining Dilemmas and Convergence Analysis

The current mining dilemma problem refers to the fact that all mining pools choose an honest mining strategy for optimal returns [35]. However, this choice may not meet the requirements of the strategy to achieve optimal returns for mining pools in different environments [36]. Currently, researchers solve this problem by modeling and simulating the mining and attacking behaviors of mining pools in different environments for multiple consensus algorithms, such as PoW and Byzantine Fault Tolerance (BFT), to solve the optimal strategy through the dynamic game approach [37]. In addition, game convergence analysis of game parameters focuses on analyzing the effects of parameter changes on convergence speed. By adjusting these parameters, convergence analysis helps mining pools mitigate revenue losses from DDoS attacks more quickly and effectively under different network conditions. Researchers have explored the dynamic convergence of various attacks, including Block Withholding (BWH) attacks, 51% attacks, and DDoS attacks.

Eyal et al. [35] proposed an evolutionary game model for a BWH attack among two mining pools to get the best mining strategy. The method analyzes the game convergence to conclude that reasonable additional reward values and penetration rates can reduce the loss of mining pools in the face of BWH attacks faster and more effectively. Chen et al. [38] proposed an evolutionary game model to solve the block size determination problem in PoW. This method analyzes the convergence rate of the game by changing the relevant parameters of the size of the optimal block and effectively analyzes the mining pool to obtain the optimal profit strategy. Ren et al. [39] proposed an evolutionary game model for 51% double-spending attacks in blockchain, revealing a dynamic evolution trend in the node strategy. The model analyzes the influence of convergence rate on a game by changing the parameter values of the transaction price and transaction cost. This analysis method can effectively deal with the risk of 51% double-spending attacks. Tang et al. [40] proposed a game-theoretic approach named the Edge DDoS Mitigation (EDM) Game for decentralized mitigation of edge DDoS attacks. This method introduces the finite improvement property for convergence analysis and proves the existence of Nash equilibria through iterative processes, ensuring the algorithm's convergence. Rathnayake et al. [41] propose Blockchain Data Trust (BDT)-Benchmark—a comprehensive synthetic dataset for ML-driven blockchain trust evaluation—which addresses the existing dataset limitations and the issues of blockchain's inability to guarantee data trustworthiness and existing dataset limitations, and supports related research.

Several dynamic game approaches exist to the mining dilemma problem in PoW. Huang et al. [42] proposed a mining dilemma solution for BWH attacks based on dynamic evolutionary games. Using the Lyapunov approach, the method can solve the optimal strategy for mining pools encountering BWH attacks under different punishments and regulatory environments. Fujita et al. [43] addressed the problem of mining pool selection in the presence of BWH attacks in a blockchain network through evolutionary game theory. The expected revenue densities of miners in different mining pools are investigated, and the evolutionary stable state (ESS) is determined by replicating the dynamic formula to analyze the stable distribution of miners in different mining pools. Zhang et al. [44] employed evolutionary game theory to study how blockchain participants adjust their cooperative behavior under different costs and benefits. Their simulations demonstrated stable cooperative strategies and revealed the influence of network structure on coop-

eration. Wang et al. [45] improved the incentive mechanism in the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism by introducing an evolutionary game theory approach to enhance the stability and security of the system. The effectiveness of the mechanism in promoting honest participation and resisting bribery attacks is verified through simulation experiments.

2.3. Challenges in Current Research

Although existing methods can detect and mitigate DDoS attacks, they still exhibit several limitations. As shown in Table 1, ML-based detection achieves high accuracy but incurs significant resource overhead and lacks long-term strategic analysis. Static game methods require no additional resources but fail to adapt to dynamic changes. Evolutionary game approaches capture long-term dynamics but suffer from either oversimplified models or incomplete convergence analysis. This paper addresses these gaps through rigorous convergence analysis and systematic parameter sensitivity evaluation.

Table 1. Comparison of Current DDoS Detection and Mitigation Methods.

Method Category	Representative Work	Main Strengths	Resource Overhead	Dynamic Adaptation	Convergence Analysis	Core Limitations
ML-based Detection	Dai et al. [29]	Accurate DDoS traffic detection	High; degrades system performance	No; lacks game-theoretic modeling	No convergence analysis	Detection only; no strategic guidance for mining pools
Static Game Models	Johnson et al. [32]	Balances attack-defense strategies	None	No; fails to capture long-term evolution	One-shot equilibrium only	Cannot guarantee stability in dynamic networks
DDoS-focused Evolutionary Games	Huang et al. [16]	Solves optimal strategies under different networks	None	Partial; over-simplified assumptions	Incomplete; lacks parameter sensitivity analysis	Insufficient adaptation to complex dynamics; no rigorous convergence guarantee
Other Attack-focused Evolutionary Games	Eyal et al. [35]	Characterizes long-term strategy evolution (BWH)	None	Partial; applicable to BWH only	Complete for BWH but not verified for DDoS	Focus on BWH; conclusions not directly transferable to DDoS

3. The Proposed DEG-Based Model

3.1. Description and Assumptions of the Blockchain System Model

The blockchain system we have established is illustrated in Figure 1. As can be seen from Figure 1, a malicious pool A launches DDoS attacks against a target pool via the networks to obtain illegal profits. We assume that the mining pool manager manages the revenue of the mining pool and identifies the attacking and honest mining pools by abnormal traffic. The pool manager determines which pool is launching a DDoS attack by the excessive amount of anomalous traffic. In Figure 1, the mining pool manager determines mining pool A by monitoring abnormal traffic. Mining pool A is identified as the mining pool that launches a DDoS attack. The attack of mining pool A causes mining pool B to be disconnected from the mining site. As a consequence of the attack, mining pool A obtains a portion of pool B's honest-mining revenue. We assume that the honest mining revenue for each pool is R . Malicious mining pool A controls n nodes to launch DDoS attacks against honest mining pool B through the blockchain networks. Thus, damage caused by each

maliciously controlled node is d , then the loss caused by n nodes to the honest mining of pool B is nd . As a result, mining pool A initiating the DDoS attacks earns an illicit mining reward of wnd . The cost of DDoS launched by mining pool A is c_2 . The pool manager penalizes pool A with c_1 over the network and rewards pool B with a for honest mining. Therefore, in this scenario, pool A earns $R + wnd - c_1 - c_2$, while pool B earns $R - wnd + a$, resulting in significant losses for the honest pool.

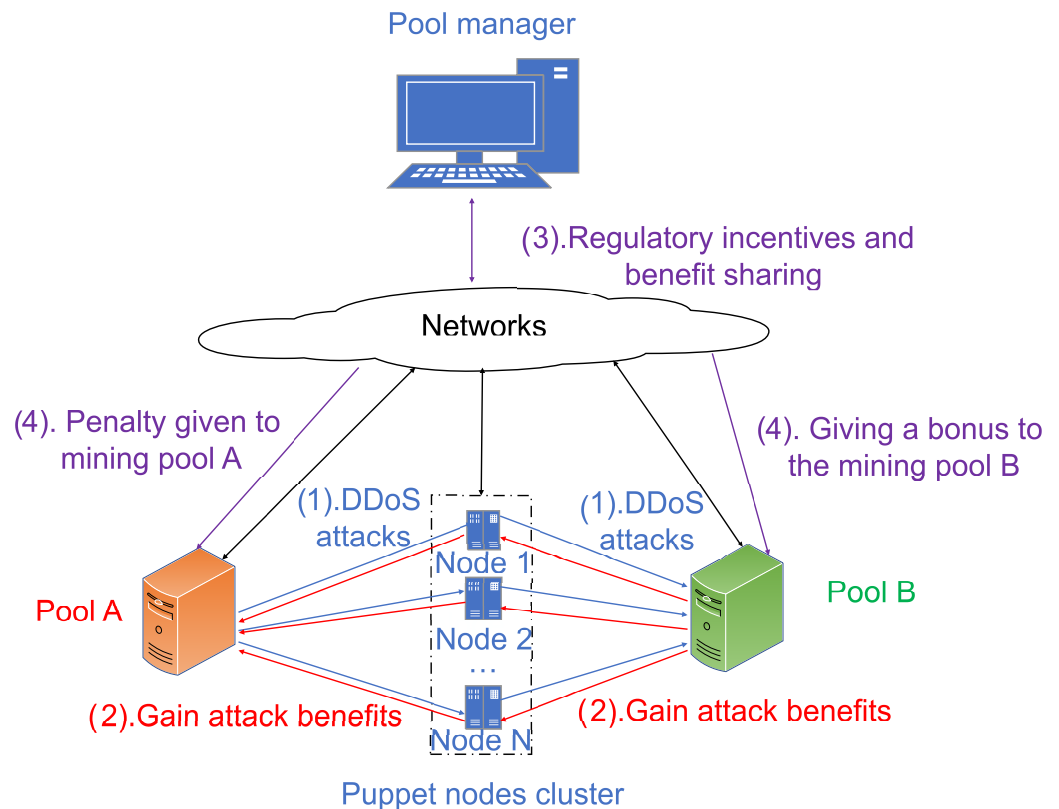


Figure 1. Mining pool DDoS attack scenario in IoT-enabled blockchain systems.

For further analysis, we employ the assumptions and parameter definitions summarized in Table 2.

(1) This paper studies two equal-power mining pools, A and B, where the manager detects attackers via abnormal traffic. The focus is on determining the optimal mining strategy when one pool launches DDoS attacks against another.

(2) The honest mining reward for both pools A and B is R , where $R > 0$.

(3) A malicious mining pool controls n nodes to launch DDoS attacks on an honest pool, each causing damage d . The total impact and illegal gain, wnd , depends on the network factor w ($0 \leq w \leq 1$), where $w = 0$ indicates a paralyzed network and $w = 1$ ideal conditions.

(4) The coefficient w is a normalized composite index representing the effectiveness of DDoS attacks under current network conditions, rather than a single raw network metric. It can be estimated by combining indicators such as packet loss rate, round-trip time, and service availability.

(5) The mining pool manager gives c_1 as a penalty for attacking the mining pool and a as a reward for honest mining. The values of c_1 and a satisfy $c_1 > 0$ and $a > 0$. The cost of launching a DDoS attack is c_2 . The value of c_2 is $c_2 > 0$.

(6) This model does not allow miners to migrate to other pools or to launch additional attacks on the mining pool.

These assumptions are introduced to obtain a tractable two-pool dynamic game model. In practical blockchain systems, heterogeneous hashrates, imperfect attacker identification, and miner migration may further affect strategy evolution.

Table 2. Modeling parameters for DEG model.

Parameter	Description
R	Reward assigned by the pool manager when a pool successfully mines a block
d	Revenue loss of the victim pool or gain by the attacker
a	Reward obtained by an honest mining pool
c_1	Penalty imposed on the attacking mining pool
c_2	Cost of launching a DDoS attack
n	Number of malicious nodes controlled by the attacker
w	Network environment coefficient(quality of network)
f_1	Return from honest mining
f_2	Return from launching DDoS attacks
$\bar{f}$	Average return under DDoS conditions
$F(x)$	Replicator dynamic function over time t
$F'(x)$	Derivative of $F(x)$ with respect to honest mining probability x
x	Probability that a mining pool mines honestly
x_i	Candidate strategies for mining pools
x^*	Optimal strategy of the mining pool

3.2. The DEG Threat Model

Our model considers two mining pools and two strategies (honest mining and launching attacks). This setting avoids the exponential growth of state variables that arises with multiple pools or strategies, which often results in simulation distortion. Additionally, this model captures the essential “profit–fairness” trade-off among mining pools, and its resulting behavioral patterns are sufficient to support the core conclusions of this work. This paper analyzes revenue profiles for mining pools under various DDoS attack scenarios, differentiating between strategies of honest mining (H) and launching DDoS attacks (D) across four potential scenarios: both pools mining honestly (H, H), pool B attacking pool A (H, D), pool A attacking pool B (D, H), and both pools attacking each other (D, D). In scenario (H, D), pool A mines honestly while pool B’s attack, controlled by n nodes and influenced by network environment factor w , yields illegal profit of wnd for pool B at the expense of pool A, offset by pool B’s attack costs c_2 and a penalty c_1 from the blockchain system, resulting in net revenues of $R - wnd + a$ and $R + wnd - c_1 - c_2$ respectively. In (D, H), the situation mirrors (H, D) with roles reversed, leading to similar revenue distributions. For (D, D), both pools attack each other, canceling out illegal gains ($wnd - wnd = 0$), and after accounting for penalties c_1 and costs c_2 , both pools earn $R - c_1 - c_2$. Figure 2 illustrates the payoff differences across four attack scenarios using a game tree structure. Based on the model, we list the rewards for mining pool A and pool B. Table 3 shows the benefits for both pools in the four DDoS attack scenarios.

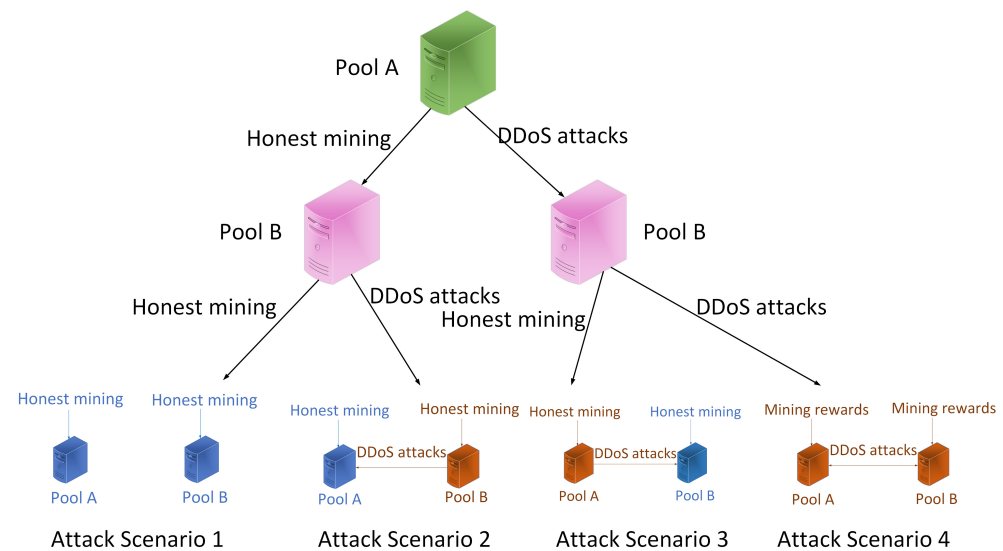


Figure 2. DDoS attack scenario diagram.

Table 3. Payoffs of mining pools under DDoS attack scenarios.

Strategy (A\B)	H	D
H	(R, R)	$(R - wnd + a, R + wnd - c_1 - c_2)$
D	$(R + wnd - c_1 - c_2, R - wnd + a)$	$(R - c_1 - c_2, R - c_1 - c_2)$

Note: H = Honest mining; D = DDoS attack; R = Honest mining revenue; n = Number of malicious nodes; d = Damage per malicious node; w = Network quality coefficient; c_1 = Penalty for DDoS attack; c_2 = Cost of launching DDoS attack; a = Reward for honest mining.

3.3. Establishment and Solution of Dynamic Equation

Figure 3 shows the complete mathematical modeling process of the proposed method. We assume the probability of honest mining is x and of launching a DDoS attack is $1 - x$, with $0 \leq x \leq 1$. The honest mining payoff is derived from Table 3 and expressed in Equation (1):

$$f_1 = x * R + (1 - x) * (R - wnd + a) \quad (1)$$

The payoff of a DDoS attack by a mining pool is expressed in Equation (2):

$$f_2 = x * (R + wnd - c_1 - c_2) + (1 - x) * (R - c_1 - c_2) \quad (2)$$

The average mining revenue of a mining pool under DDoS attack is shown in Equation (3):

$$\bar{f} = x * f_1 + (1 - x) * f_2 \quad (3)$$

Therefore, the replication dynamics of mining pool strategies can be formulated as Equation (4) [40]. Solving this equation enables us to analyze strategy evolution and identify optimal responses to DDoS attacks under different network environments. Wherein, $x(t)$ denotes the function of the change in strategy x in the case of a change at time t . dx/dt implies that the representation strategy x is the rate of change of frequency over time of t . f_1 represents the average return from honest mining in the pool. $\bar{f}$ denotes the average return of the mining pool in the presence of both a DDoS attack strategy and an honest mining strategy [46]. Equation (4) replicates the derivation of the dynamic equations and the optimal strategy solution. See the theorem on evolutionary games in Ref. [47].

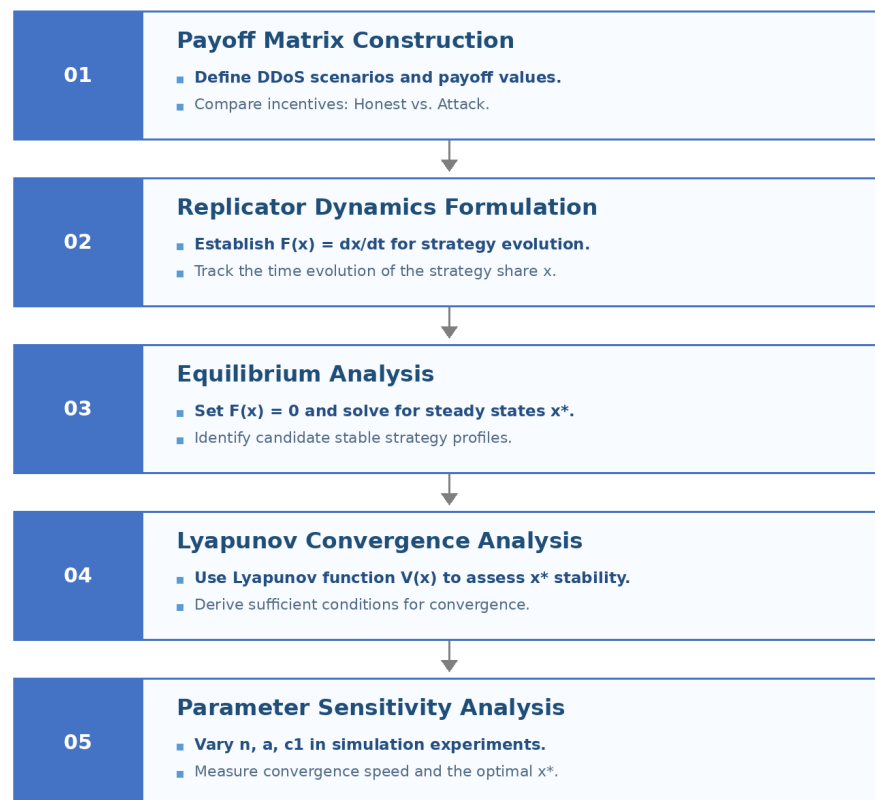


Figure 3. Modeling Framework of the Proposed DEG-based Method.

$$\begin{aligned}
 F(x) &= dx(t)/dt \\
 &= x(f_1 - \bar{f}) \\
 &= x * \{f_1 - [x * f_1 + (1 - x) * f_2]\} \\
 &= x[f_1 - x * f_1 - (1 - x) * f_2] \\
 &= x[(1 - x)f_1 - (1 - x) * f_2] \\
 &= x(1 - x)(f_1 - f_2) \\
 &= x(1 - x)[(c_1 + c_2 - w * n * d)x + \\
 &\quad (1 - x)(a - w * n * d + c_1 + c_2)] \\
 &= x(1 - x)(c_1 + c_2 + a - w * n * d - ax)
 \end{aligned} \tag{4}$$

Setting $F(x) = 0$ yields the three candidate stationary points of the evolutionary game shown in Equation (5):

$$x_1 = 0, x_2 = 1, x_3 = \frac{c_1 + c_2 + a - wnd}{a} \tag{5}$$

By solving the replication dynamic equation in Equation (4), we obtain three candidate stationary points x_i ($i = 1, 2, 3, \dots$). Among them, $x_1 = 0$ and $x_2 = 1$ are trivial boundary equilibria, while the interior solution $x_3 \in (0, 1)$ requires stability validation rather than being directly regarded as a stable evolutionary state.

To judge whether x_3 is an evolutionarily stable strategy (ESS), we first compute the derivative of $F(x)$ from Equation (4):

$$\begin{aligned}
 F'(x) &= \frac{d}{dx}[x(1 - x)(c_1 + c_2 + a - wnd - ax)] \\
 &= (1 - 2x)(c_1 + c_2 + a - wnd - ax) - ax(1 - x)
 \end{aligned}$$

By definition, x_3 is the point where $c_1 + c_2 + a - wnd - ax_3 = 0$. Substituting this into the expression for $F'(x_3)$ yields

$$\begin{aligned} F'(x_3) &= (1 - 2x_3) \cdot 0 - ax_3(1 - x_3) \\ &= -ax_3(1 - x_3) \end{aligned}$$

According to the linearization stability criterion for one-dimensional autonomous dynamical systems, an interior equilibrium x^* is locally asymptotically stable if the derivative of the replicator dynamics satisfies $F'(x^*) < 0$ [48]. Since the basic assumptions of our model satisfy $a > 0$ and $0 < x_3 < 1$, we have $F'(x_3) < 0$, confirming local asymptotic stability around x_3 .

Then we define the four payoff entries of the symmetric two-strategy game as

$$\alpha = R, \beta = R - wnd + a, \gamma = R + wnd - c_1 - c_2, \delta = R - c_1 - c_2.$$

For a symmetric two-strategy game, an interior equilibrium can become a mixed-strategy ESS only if the discriminant condition below is satisfied [49]:

$$\alpha - \beta - \gamma + \delta < 0$$

Substituting the model payoffs into this formula and simplifying, we can derive that

$$\alpha - \beta - \gamma + \delta = -a.$$

Since $a > 0$ by assumption, we have $-a < 0$, this condition is satisfied.

Therefore, x_3 is a valid ESS only when it falls within the range $0 < x_3 < 1$.

Following the reference in [50], we evaluate the optimal strategy x^* under varying network conditions and determine the corresponding network coefficient w . On this basis, we adopt evolutionary game theory to analyze the convergence behavior of strategies and explore the parameter sensitivity of key variables, including the malicious node count n , reward a , and penalty c_1 .

4. Optimal Strategy Solution and Convergence Analysis

This section analyzes stability and convergence via replicator dynamics and equilibrium analysis, combined with Lyapunov stability theory. We adopt the Lyapunov function $V(x) = \frac{1}{2}(x - x^*)^2$ [51] to analyze the stability of the interior equilibrium $x_3 \in (0, 1)$ and solve the optimal mining strategy x^* , we regard the network coefficient w as the key influencing factor. We only calculate the sign of $\dot{V}(x)$ for Case C, which verifies the global asymptotic stability for all initial states within the open interval $(0, 1)$. This stability conclusion does not hold for the invariant boundary points $x = 0$ and $x = 1$. For the boundary optimal solutions $x^* = 0$ (Case A) and $x^* = 1$ (Case B), we further evaluate their local asymptotic stability by computing the first derivative of the replicator dynamics $F'(x)$ at the boundary equilibria. Under the prerequisites $a > 0$ and $c_1 > 0$, we finally derive the stable optimal strategies corresponding to Case A, Case B, and Case C based on the three stationary points x_1 , x_2 , and x_3 . Furthermore, we conduct parameter sensitivity analysis to explore how the penalty coefficient c_1 , the honest mining reward a , and the number of malicious nodes n affect the strategy convergence speed. Figures 4–6 show phase diagrams of replicator dynamics $F(x) = \frac{dx(t)}{dt}$ under different networks, and parameters are detailed in Table 4.

Case A: $a > 0$ and $x_3 = \frac{c_1 + c_2 + a - wnd}{a} \leq 0$.

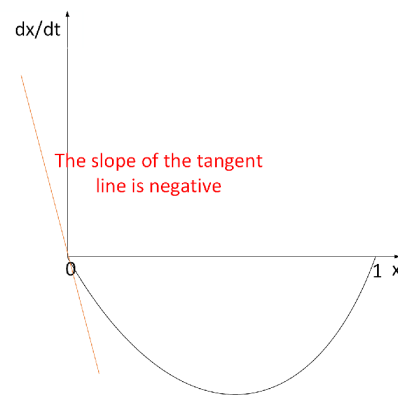


Figure 4. The replicator-dynamics phase diagram for case A.

When $x_3 = \frac{c_1+c_2+a-wnd}{a} \leq 0$, i.e., $c_1 + c_2 + a - wnd \leq 0$, the network coefficient w satisfies $\frac{c_1+c_2+a}{nd} \leq w \leq 1$ ($nd > 0$). By analyzing the first derivative $F'(x)$ of the replication dynamic equation $F(x)$, the steady state corresponds to the intersection with the horizontal axis where the slope is negative ($F'(x) < 0$) [38,39,52]. The phase diagram in Figure 4 shows that the stable strategy in this case is $x^* = x_1 = 0$, indicating that under good network conditions, mining pools eventually choose mutual attacks to maximize profits.

Then, we consider how the variable parameters a , c_1 , and n affect the convergence time to the optimal strategy in repeated games among mining pools with different mining probabilities. By assumption, the range of a is $0 < a \leq wnd - c_1 - c_2$. Similarly, we have $n \geq \frac{c_1+c_2+a}{wd}$ ($wd > 0$) and $0 < c_1 \leq wnd - a - c_2$. Under these conditions, n tends to be relatively large, while a and c_1 are relatively small. Therefore, given the same penalty c_1 and reward a , a larger number of attacking nodes n controlled by the malicious mining pool leads to faster game convergence. Conversely, with a fixed n , higher penalty c_1 , and reward a slow down the convergence of the mining pool game.

Case B: $a > 0$ and $x_3 = \frac{c_1+c_2+a-wnd}{a} \geq 1$

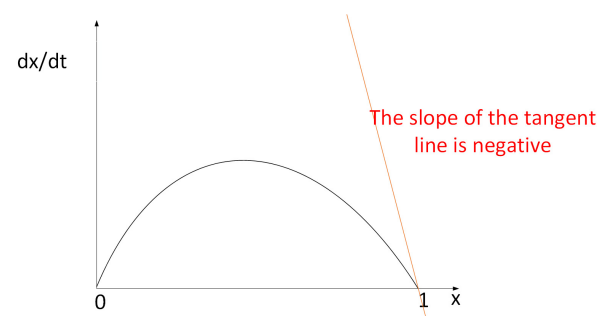


Figure 5. The replicator-dynamics phase diagram for case B.

When $x_3 = \frac{c_1+c_2+a-wnd}{a} \geq 1$ means $c_1 + c_2 + a - wnd \geq a$. In this case, the value range of w is $0 \leq w \leq \frac{c_1+c_2}{nd}$ ($nd > 0$). The replication dynamic phase diagram is shown in Figure 5. From Figure 5, we conclude that the stable strategy point with $F'(x) < 0$ is $x_2 = 1$. Thus, the steady-state strategy is $x^* = 1$. Under poor network conditions, mining pools tend to mine honestly to secure optimal rewards before suffering from DDoS attacks.

Then, we analyze how the variable parameters a , c_1 , and n affect convergence to the optimal strategy in Case B. According to Case B assumptions, the number of malicious nodes n satisfies $0 < n \leq \frac{c_1+c_2}{wd}$ ($wd > 0$). Similarly, the reward a and penalty c_1 satisfy $a > 0$ and $c_1 \geq wnd - c_2$. In this scenario, n tends to be relatively small, while a and c_1 are relatively large. Therefore, under the same poor network condition w , penalty c_1 , and reward a , a larger number of attacking nodes controlled by the malicious pool slows game

convergence. Conversely, with fixed w and n , higher penalty c_1 and reward a accelerate convergence, reducing the time for the mining pool to reach the optimal strategy.

Case C: $a > 0$ and $0 < \frac{c_1+c_2+a-wnd}{a} < 1$

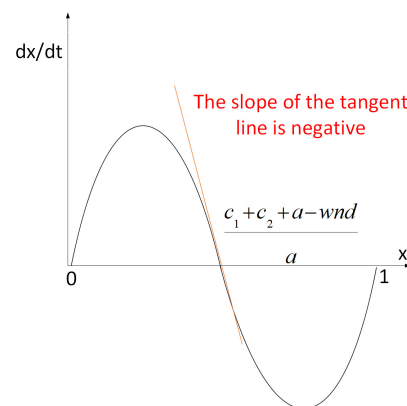


Figure 6. The replicator-dynamics phase diagram for case C.

Table 4. Parameter ranges under different strategies x^* .

Parameter	$x^* = x_1 = 0$	$x^* = x_2 = 1$	$x^* = x_3 = \frac{c_1 + c_2 + a - wnd}{a}$
R	$R > 0$	$R > 0$	$R > 0$
a	$0 < a \leq wnd - c_1 - c_2$	$a > 0$	$a > \max(wnd - c_1 - c_2, 0)$
d	$d > 0$	$d > 0$	$d > 0$
c_1	$0 < c_1 \leq wnd - a - c_2$	$c_1 \geq wnd - c_2$	$wnd - a - c_2 < c_1 < wnd - c_2$
c_2	$c_2 > 0$	$c_2 > 0$	$c_2 > 0$
n	$n \geq \frac{c_1 + c_2 + a}{wd}$	$0 < n \leq \frac{c_1 + c_2}{wd}$	$\frac{c_1 + c_2}{wd} < n < \frac{c_1 + c_2 + a}{wd}$
w	$\frac{c_1 + c_2 + a}{nd} \leq w \leq 1$	$0 \leq w \leq \frac{c_1 + c_2}{nd}$	$\frac{c_1 + c_2}{nd} \leq w \leq \frac{c_1 + c_2 + a}{nd}$

In this case, the value range of w is as follows: $\frac{c_1+c_2}{nd} \leq w \leq \frac{c_1+c_2+a}{nd}$ ($nd > 0$). The replication dynamic phase diagram is shown in Figure 6. As can be seen from Figure 6, the steady-state strategy point that makes $F'(x) < 0$ chosen in case C is $x^* = x_3 = \frac{c_1+c_2+a-wnd}{a}$ ($a > 0$). Under the condition of the medium network environment, the mining pool will choose the probability of honest mining as $x_3 = \frac{c_1+c_2+a-wnd}{a}$ to obtain the best profits. When the network environment is in a relatively stable state, the mining pools will eventually choose the mixed strategy for the best profit. The pools are finally mined honestly with a probability of $x_3 = \frac{c_1+c_2+a-wnd}{a}$.

In Case C, the variable parameters a , c_1 , and n influence both the convergence speed and the mining pool's mixed strategy x^* . The number of malicious nodes satisfies $\frac{c_1+c_2}{wd} < n < \frac{c_1+c_2+a}{wd}$ ($wd > 0$), indicating a moderate level of control. The penalty and reward ranges are $wnd - a - c_2 < c_1 < wnd - c_2$ and $a > \max(wnd - c_1 - c_2, 0)$. Increasing a tends to increase c_1 , with both similarly affecting convergence speed. For fixed n , higher a and c_1 accelerate convergence; increasing n with fixed a and c_1 slows it. The optimal mixed strategy is given by $x_3 = \frac{c_1+c_2+a-wnd}{a}$, which decreases as n grows. At fixed n and network coefficient w , increasing a and c_1 raises x_3 and speeds convergence. The values of these parameters work together to determine convergence and strategy selection.

5. Experiment and Results

5.1. Simulation Configuration and Interpretation of Evolutionary Time

(1) Simulation Configuration: All simulations were conducted in MATLAB R2025a (version 25.1.0, The MathWorks, Inc., Natick, MA, USA). The replicator dynamics modeled by ordinary differential equations (ODEs) are solved via the ode45 solver. For each scenario, we simulated the evolution of the strategy from a set of initial honest mining probabilities, x , ranging from 0.1 to 0.9 in steps of 0.1.

(2) Interpretation of the Time Variable t : In our experiment, it describes the continuous strategy adjustment process inherent to the replicator dynamics model, where the time scale is determined by the relative rates of strategy change, independent of real mining system operations. Notably, throughout this paper, the variable t in all figures and reported convergence times (e.g., “0.5 s”, “0.03 s”) represents normalized evolutionary time, not physical wall-clock time.

(3) Definition of Convergence Time: In the simulations, convergence time is defined as the normalized time T_ε :

$$T_\varepsilon = \inf \{t : |x(t) - x^*| < \varepsilon\},$$

where the strategy state remains within this threshold for all subsequent time steps, and the tolerance parameter is set to $\varepsilon = 10^{-3}$.

(4) Mapping to Real Time: While t is abstract, it can be mapped to physical time if we specify a strategy update interval Δ . If mining pools update their strategies every Δ s, the real convergence time can be formulated as $T_{\text{real}} = T_{\text{sim}}\Delta$. Here, Δ can correspond to a traffic-monitoring window, a block-generation interval, or a pool-management decision interval.

5.2. Dynamic and Static Comparison Experiment

This section validates the proposed DEG model by comparing it with the static DDoS policy [16] using Johnson’s game model [32]. It is important to clarify that the comparison does not aim for identical parameter replication, but focuses on the analytical differences between static and dynamic models. Our DEG model includes extra practical parameters (e.g., attack cost c_2) that are absent in static models. Given the inherent structural differences between the two model frameworks, we adopt respective parameter configurations to maintain conceptually equivalent network scenarios for the logical fairness of the comparison.

The experiment clearly highlights the superiority of our DEG model. Static models can only identify a final equilibrium; they fail to capture the evolutionary path and convergence speed of strategy adjustment. Although our previous work made progress, it did not fully analyze how key parameters affect this process. Our current work addresses these limitations. It clearly tracks strategy convergence trends. It also reveals how key parameters, including n , a and c_1 , influence the entire evolutionary process. Moreover, static models cannot provide definite results for optimal mixed strategies. In contrast, our model calculates the precise optimal strategy probabilities and reflects the real adaptive behaviors of mining pools facing DDoS attacks. The specific experimental parameters are shown in Table 5.

The comparison experiment consists of three parts: harsh, medium, and good network conditions, using both static and dynamic games to determine optimal mining pool strategies under DDoS attacks. This section compares dynamic game results from previous work [16] with the current dynamic and additional static game experiments. Static game results are presented as 3D plots with mining pool A and pool B strategies on the x- and y-axes and revenues on the z-axis; blue points represent non-equilibrium states, while red points indicate optimal equilibria. Dynamic game results show colored curves of mining

pools' initial honest mining probabilities (ranging from 0.1 to 0.9) over time, illustrating convergence to optimal strategies in each network environment.

Table 5. Experimental parameter settings.

R	a	d	c_1	c_2	n	w	Optimal x^*
300	30	10	20	10	25	0.1	$x^* = x_2 = 1$ for current work
300	30	10	20	10	8	0.5	$x^* = x_3 = 0.67$ for current work
300	30	10	20	10	25	0.9	$x^* = x_1 = 0$ for current work
200	30	60	20	–	–	0.1	$x^* = 1$ for previous work
200	30	60	20	–	–	0.5	$x^* = 0.67$ for previous work
200	30	60	20	–	–	0.9	$x^* = 0$ for previous work

5.2.1. The Harsh Network Comparison Experiments

In this experiment, the network environment coefficient is set to $w = 0.1$ to represent harsh network conditions. Consistent with our previous work [16], we adopt the basic parameter settings of reward $a = 30$ and penalty $c_1 = 20$. Differently, this paper additionally considers the attack cost $c_2 = 10$, which is neglected in the static model. For network scenario differentiation, we configure the number of malicious nodes as $n = 8$ for medium network environments, and $n = 25$ for harsh and good network environments. All experimental parameters used for model comparison are summarized in Table 5. The corresponding static and dynamic game experimental results are presented in Figure 7.

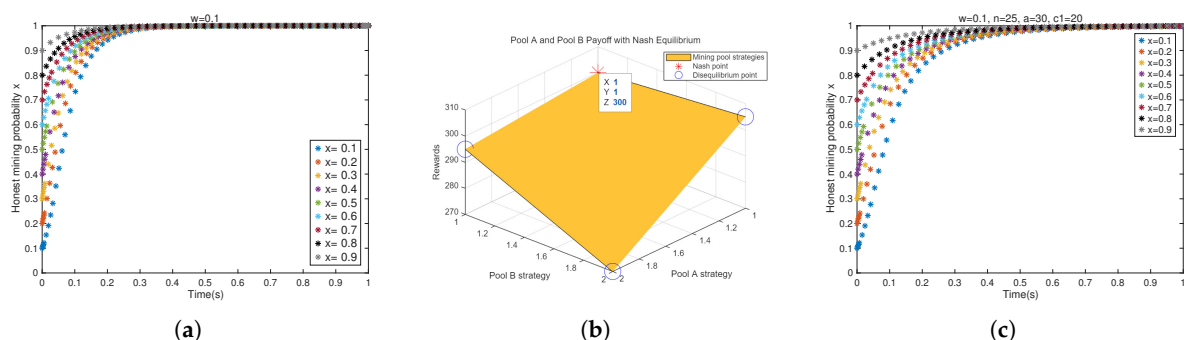


Figure 7. Dynamic and static comparison experiments in harsh network environments. (a) Experimental results of dynamic games in previous work. (b) The static game experiment in the current work. (c) Experimental results of dynamic games in the current work.

Figure 7a presents the dynamic game results from our previous work. In a harsh network environment, mining pools quickly converge to the strategy $x^* = 1$ within 0.3 s, which verifies that honest mining is the optimal strategy in this scenario. Figure 7b displays the static game results of this study under the same harsh network condition. The optimal equilibrium is (1, 1, 300). Both mining pools choose honest mining to achieve a maximum revenue of 300. Figure 7c illustrates the dynamic evolutionary game results of the proposed model with the parameter settings in Table 5. After iterative game evolution, all mining pools converge steadily to $x = 1$ at approximately 0.4 s. This outcome demonstrates that honest mining ($x^* = 1$) remains the unique optimal strategy under harsh network environments.

In adverse network environments, mining pools are unable to observe or predict the strategies of other pools. In this case, DDoS attacks bring high uncertainty and risk, so mining pools prefer honest mining. Worse network conditions reduce the attack-

related gain wnd , while the attack costs c_2 and penalties c_1 stay unchanged. This makes attacks unprofitable.

5.2.2. The Medium Network Comparison Experiments

The parameter settings of our previous work [16] are retained as baseline: $w = 0.5$, $c_1 = 20$, $a = 30$, $d = 60$, and $R = 200$. For the medium network experiments in this study, we adjust the number of malicious nodes to $n = 8$, $d = 10$ and $R = 300$, while keeping all other parameters consistent with the baseline. Figure 8 presents the static and dynamic game results of mining pool strategy evolution under this medium network scenario.

Figure 8a presents previous dynamic game results showing that in moderate network environments, the optimal strategy is a mixed policy with honest mining probability $x^* = 0.67$. Figure 8b illustrates static game results, yielding two optimal strategies for pool A: $(1, 2, 290)$ and $(2, 1, 310)$, corresponding to role-swapped equilibria (H, D) and (D, H) . Under (H, D) , pool A's payoff is $R - wnd + a = 300 - 0.5 \times 8 \times 10 + 30 = 290$, while pool B's is $R + wnd - c_1 - c_2 = 300 + 40 - 20 - 10 = 310$. Conversely, under (D, H) , pool A's payoff is 310 and pool B's is 290. These results suggest mining pools adopt mixed strategies balancing honest mining and attacks. Figure 8c demonstrates dynamic evolutionary game convergence, where initial honest mining probabilities (0.1 to 0.9) converge to $x = 0.67$ around $t = 0.5$ s. This aligns with the theoretical equilibrium $x_3 = \frac{c_1 + c_2 + a - wnd}{a} = \frac{20 + 10 + 30 - 0.5 \times 8 \times 10}{30} = 0.67$. Thus, under moderate network conditions, mining pools converge to a mixed strategy with honest mining probability $x^* \approx 0.67$, balancing profitable attack opportunities with honest mining returns.

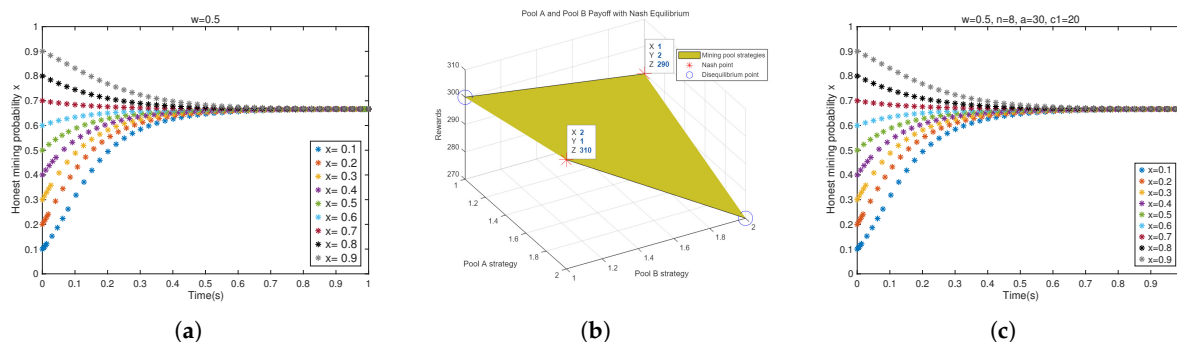


Figure 8. Dynamic and static comparison experiments in medium network environments. (a) Experimental results of dynamic games in previous work. (b) The static game experiment in the current work. (c) Experimental results of dynamic games in the current work.

In medium network environments, mining pools adopt an optimal mixed strategy that balances honest mining and DDoS attacks. When the network coefficient w rises from 0.1 to 0.5, DDoS attack profits increase, motivating mining pools to adopt aggressive strategies. However, penalty c_1 and attack cost c_2 constrain malicious behaviors. This trade-off produces multiple optimal strategies. Experimental results confirm that the optimal mixed strategy for all pools features an honest mining probability of $x^* = 0.67$.

5.2.3. The Good Network Comparison Experiments

To simulate a favorable network condition, this experiment sets the network coefficient to $w = 0.9$ and the number of malicious nodes $n = 25$. Such settings construct an optimal and stable network environment. All other experimental parameters follow the configurations in Table 5. Figure 9 illustrates the static and dynamic game experimental results of mining pools under this favorable network condition.

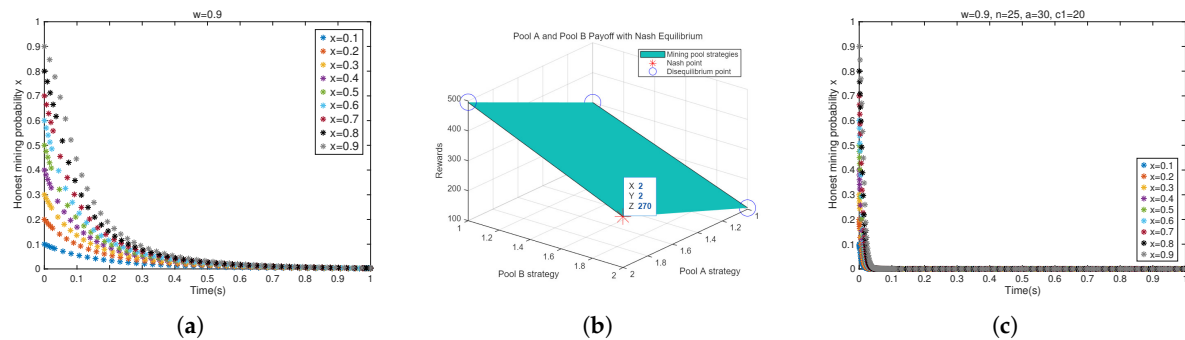


Figure 9. Dynamic and static comparison experiments in good network environments. (a) Experimental results of dynamic games in previous work. (b) The static game experiment in the current work. (c) Experimental results of dynamic games in the current work.

Figure 9a shows the experimental results of previous work, where mining pools can obtain profitable gains by launching DDoS attacks under good network conditions. The static game experiment results of the current work are shown in Figure 9b. These results demonstrate that the Nash equilibrium of pool A and pool B is (2, 2, 270) in good network environments. This outcome indicates that both pools choose to launch DDoS attacks against each other to achieve an optimal gain of 270. Figure 9c presents the dynamic game experiment results of the current work in the same good network environment. The results show that, regardless of their initial strategies, the mining pools' honest mining probabilities all rapidly converge to 0 within approximately 0.03 s. This proves that the optimal strategy for the mining pools in this setting is $x^* = 0$. In summary, these experiments consistently show that under good network conditions, all mining pools will opt to launch DDoS attacks against each other to maximize their profits.

In both current and previous works, mining pools tend to maximize profits by launching DDoS attacks in good network environments. As the network improves, pools perceive attacks as more profitable than honest mining, leading them to favor DDoS strategies. The illicit gains represented by wnd and wd increase with the network coefficient. For instance, they rise from $w = 0.5$ in medium networks to $w = 0.9$ in good network conditions, which further incentivizes attacks.

5.3. Game Convergence Analysis Experiments

This section evaluates mining pools' response speed and sensitivity to DDoS attacks by varying the penalty c_1 , reward a , and number of malicious nodes n . Rapid convergence is crucial for reducing revenue loss. Three experiments are conducted using the parameter settings in Tables 6–8, which align with the optimal ranges derived from the Lyapunov analysis. Extended parameter traversal and equilibrium validation are given in Appendix A.

Table 6. Parameters for convergence and sensitivity analysis in harsh network environments.

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	20	10	15	10	5	0.1	$x^* = x_2 = 1$
300	20	10	15	10	20	0.1	$x^* = x_2 = 1$
300	30	10	20	10	5	0.1	$x^* = x_2 = 1$
300	30	10	20	10	20	0.1	$x^* = x_2 = 1$

5.3.1. The Harsh Network Game Convergence Experiments

This section explores how the penalty c_1 , reward a , and malicious node number n affect the convergence speed and game sensitivity of mining pools. All experiments are conducted under harsh network conditions with $w = 0.1$. The detailed parameter configurations are listed in Table 6. The baseline parameters are set as $c_1 = 15$, $a = 20$, and $n = 5$. We design three groups of comparative experiments. First, we increase n to 20 while keeping c_1 and a unchanged. Second, we adjust all three parameters to $c_1 = 20$, $a = 30$, and $n = 5$. Third, we set $a = 30$, $c_1 = 20$, and $n = 20$. These groups clarify the individual effects of n , c_1 , and a on strategy convergence, and the corresponding results are presented in Figure 10.

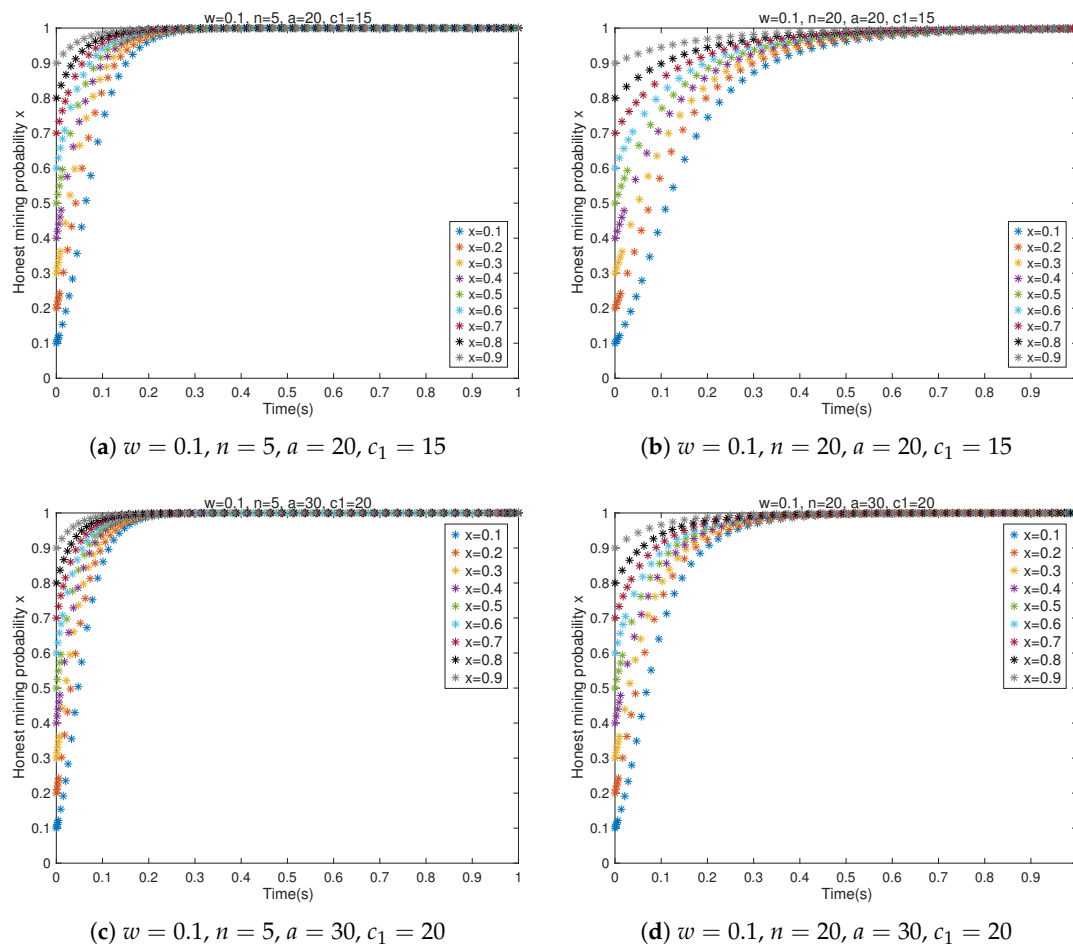


Figure 10. Game convergence experiments in harsh network environments.

Specifically, we first analyze the convergence speed and sensitivity of the game, with a focus on the variable parameter n . The results are shown in Figure 10a,b. In this group, parameters a and c_1 are fixed, while the value of n changes from 5 to 20. All mining pools adopting rate-based strategies finally converge to $x = 1$. As the number of malicious nodes n increases, the strategy convergence time grows longer. Figure 10c,d present another group of experimental results with $a = 30$ and $c_1 = 20$. These results show a consistent trend. In harsh network environments, more malicious nodes slow down the game convergence rate and reduce game sensitivity. We further test the impacts of parameters a and c_1 with n fixed at 5 and 20. When a rises from 20 to 30 and c_1 rises from 15 to 20, the mining pool strategy converges faster to the optimal value $x = 1$. The comparison results across Figure 10a–d clearly verify this conclusion. It demonstrates that increasing c_1 and a can improve the convergence speed and game sensitivity under fixed harsh network conditions. These

findings are consistent with the parameter sensitivity analysis of Case B in Section 4, which further verifies the accuracy and effectiveness of the proposed model.

In harsh networks, the convergence speed to fully honest mining state is largely influenced by economic incentives. A larger number of attack nodes n tends to slow convergence because the higher potential attack reward (wnd) continuously tempts mining pools, weakening the evolutionary pressure to be honest even if attacks are ultimately unprofitable. Conversely, higher honesty rewards a and attack penalties c_1 generally accelerate convergence, as positive incentives and punitive constraints jointly push pools to abandon attacks more quickly.

For system designers, economic regulation serves as an efficient security solution. Reasonable penalties and explicit honest rewards can make attacks economically undesirable. Notably, a large n may sustain system instability even when attacks yield no profit. Therefore, well-designed economic incentive mechanisms are essential for the network to quickly restore its secure and stable state.

5.3.2. The Medium Network Game Convergence Experiments

At a network environment coefficient w of 0.5, four groups of sub-experiments are conducted to explore the convergence speed and game sensitivity by adjusting the reward, penalty, and malicious node number. The detailed parameter settings are listed in Table 7. The baseline parameters are set as $a = 20$, $c_1 = 15$, and $n = 7$. We first increase the malicious node number to $n = 9$ while keeping a and c_1 unchanged. Afterwards, we raise the reward to $a = 30$ and the penalty to $c_1 = 20$, and test two scenarios with $n = 7$ and $n = 9$, respectively.

Table 7. Parameters for convergence and sensitivity analysis in medium network environments.

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	20	10	15	10	7	0.5	$x^* = x_3 = 0.5$
300	20	10	15	10	9	0.5	$x^* = x_3 = 0.05$
300	30	10	20	10	7	0.5	$x^* = x_3 = 0.833$
300	30	10	20	10	9	0.5	$x^* = x_3 = 0.5$

The results in Figure 11 show that increasing malicious nodes from 7 to 9 prolongs the convergence time. More malicious nodes n slow down the game convergence. In contrast, higher rewards a and penalties c_1 effectively accelerate the convergence process. As the number of malicious nodes grows, mining pools tend to adopt more aggressive strategies, while increased rewards and penalties reduce their willingness to attack. These results verify that the proposed model is sensitive to key parameters in medium network environments, which is consistent with the theoretical analysis of Case C in Section 4.

In medium networks, the system typically stabilizes at a mixed strategy equilibrium $x_3 = \frac{c_1 + c_2 + a - wnd}{a}$ where mining pools balance the profits and risks of launching attacks. A larger number of malicious nodes n increases the potential attack revenue wnd , makes attacking more attractive, and reduces the equilibrium value x_3 . This balance weakens the evolutionary advantage of honest mining and thus slows down the convergence. In contrast, higher reward a and penalty c_1 raise x_3 by improving the benefits of honest behavior. Such parameter adjustments enlarge the payoff gap between different strategies, generate stronger evolutionary pressure, and effectively accelerate the convergence process.

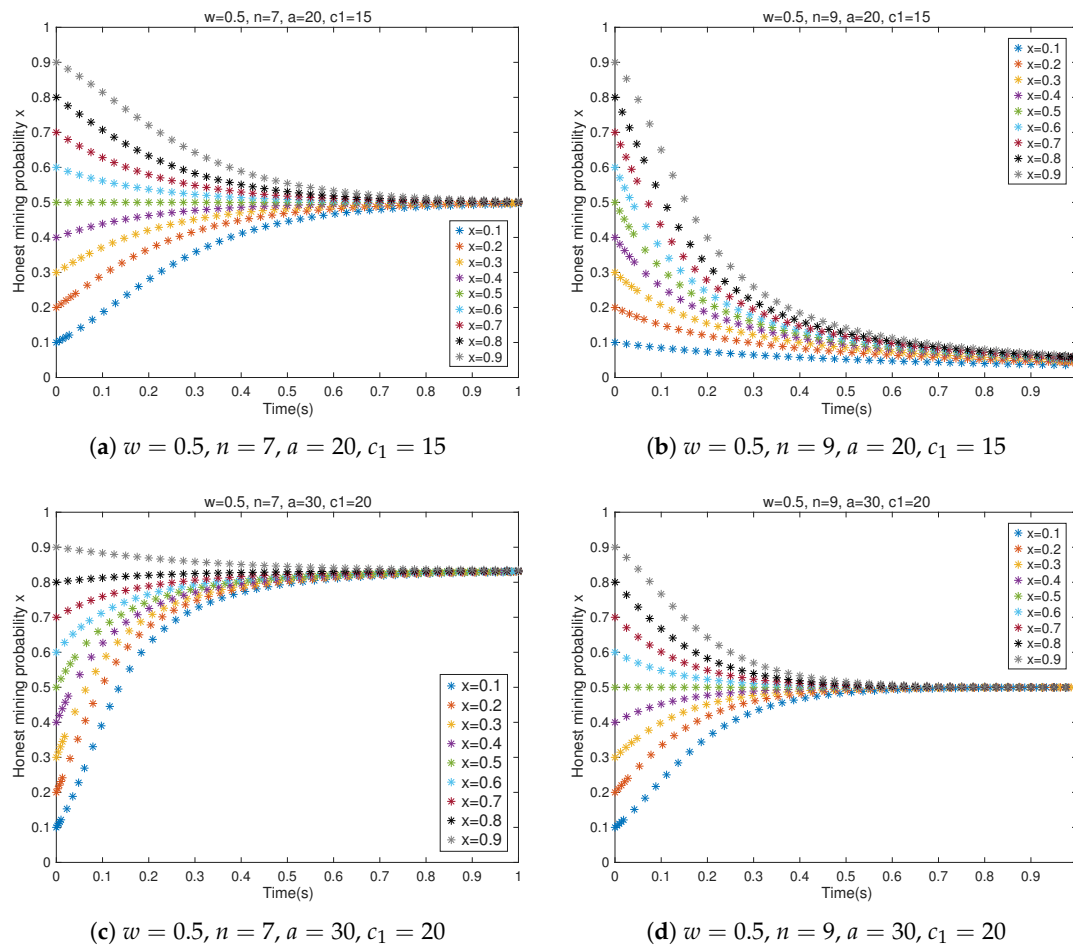


Figure 11. Game convergence experiments in medium network environments.

For system designers, these findings emphasize the necessity of active economic governance. Appropriately increasing a and c_1 can guide the system toward a safer and more stable honest mining state. In addition, a larger n drives the system toward aggressive strategies. Therefore, security parameters should be dynamically adjusted. When n increases, corresponding adjustments of a and c_1 are required to offset potential network threats and maintain stability.

5.3.3. The Good Network Game Convergence Experiments

As detailed in Table 8, several global parameters, including the honest mining reward R , attack cost c_2 , and single-node attack return d , are fixed. The network environment coefficient is set to $w = 0.9$, which represents a favorable network scenario where mining pools can obtain considerable economic benefits from DDoS attacks. We design four groups of experiments with different parameter combinations, as listed in Table 8. The baseline configuration adopts $a = 20$, $c_1 = 15$ and $n = 10$. The second group retains the same reward and penalty values but increases the number of malicious nodes to $n = 20$. The third group adjusts the parameters to $a = 30$, $c_1 = 20$ and $n = 10$. The last group sets $a = 30$, $c_1 = 20$ and $n = 20$ under favorable network conditions. The corresponding results of game convergence and parameter sensitivity analysis are presented in Figure 12.

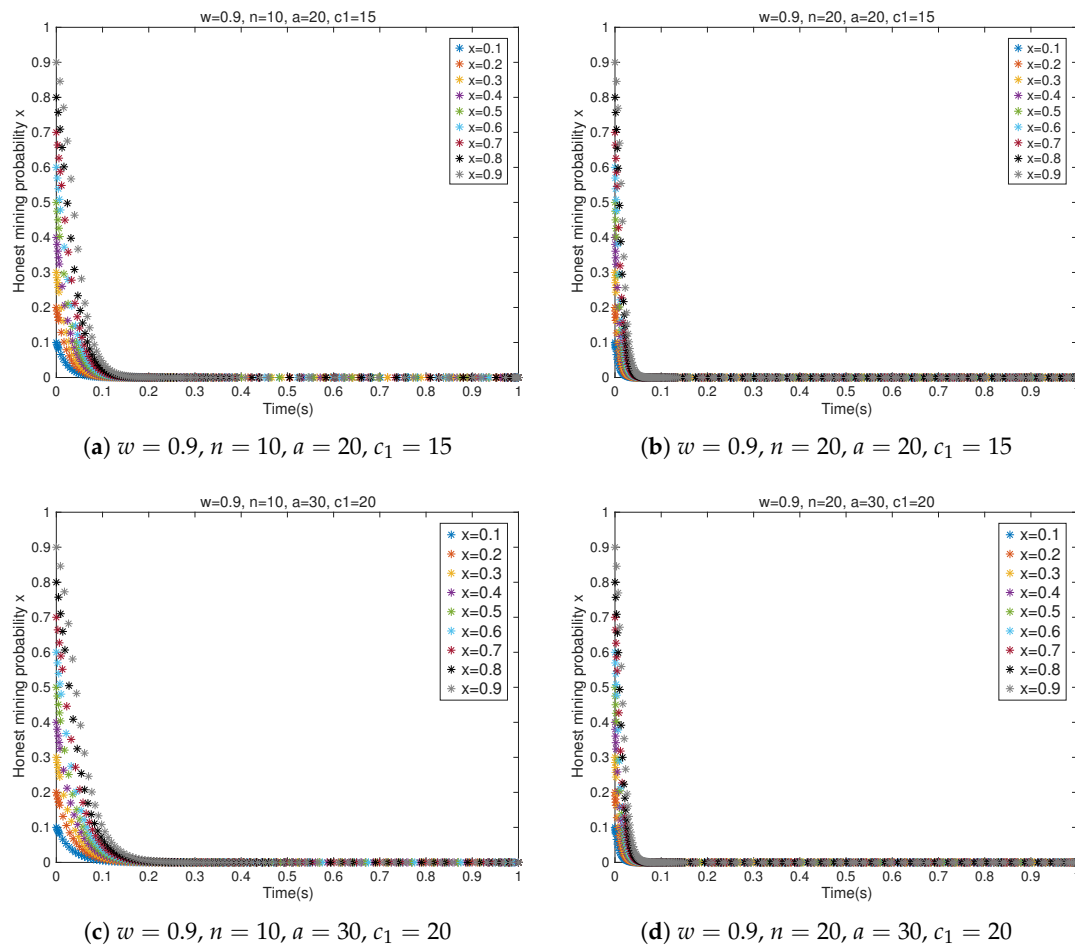


Figure 12. Game convergence experiments in good network environments.

Table 8. Parameters for convergence and sensitivity analysis in good network environments.

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	20	10	15	10	10	0.9	$x^* = x_1 = 0$
300	20	10	15	10	20	0.9	$x^* = x_1 = 0$
300	30	10	20	10	10	0.9	$x^* = x_1 = 0$
300	30	10	20	10	20	0.9	$x^* = x_1 = 0$

We conduct two groups of comparative experiments under this favorable network environment. The first group keeps the penalty c_1 and reward a unchanged and only adjusts the number of attack nodes n . The second group fixes n and varies c_1 and a . These experiments aim to explore the effects of key parameters on the game convergence performance. First, we analyze the convergence speed and parameter sensitivity by increasing n while keeping c_1 and a constant. By comparing the experimental results in Figure 12a,b under $c_1 = 15$ and $a = 20$, as well as Figure 12c,d under $c_1 = 20$ and $a = 30$, we observe that increasing n from 10 to 20 significantly accelerates the iteration process and shortens the system convergence time. In the second group of experiments, we fix n and adjust a and c_1 to explore their impacts on parameter sensitivity. A comparison between Figure 12a,c shows that increasing a and c_1 under $n = 10$ prolongs the convergence time toward the optimal strategy and reduces the model sensitivity. The same trend can be observed by comparing Figure 12b,d under $n = 20$. All experimental results are consistent with the

theoretical analysis of Case A in Section 4, which verifies the correctness and effectiveness of the proposed model and sensitivity analysis.

In favorable network environments, attack profits are far higher than honest mining gains, so the system quickly converges to the all-attack state where $x^* = 0$. The convergence speed depends on the gap between attack and honest incentives. More malicious nodes n or lower values of c_1 and a make attacks much more profitable. This creates extremely strong evolutionary pressure, causing all pools to abandon honest mining and adopt attack strategies almost instantly. In contrast, higher c_1 and a restrain this negative trend. They reduce the profit gap between honest and attack strategies, and delay the convergence process, although they cannot fully prevent aggressive behaviors.

For designers, this provides two clear guidelines. First, security mechanisms must adapt to network conditions. As the network coefficient w increases, the penalty c_1 should be correspondingly increased. Second, slowing system degradation is a practical and effective defense strategy. Even if it is difficult to restore an honest mining state, appropriately increasing rewards and penalties can delay the deterioration process. This provides sufficient time for manual intervention and defense upgrades, making it harder for the system to evolve into a dangerous attack-dominant state.

5.4. Analysis of the Effect of Network Coefficient w

To isolate and rigorously analyze the pure effect of the network environment coefficient w on strategy evolution, we conducted a set of controlled experiments. In this analysis, all other parameters were held constant ($R = 300$, $n = 15$, $d = 10$, $a = 30$, $c_1 = 20$, and $c_2 = 10$), while w was systematically varied across the values [0.1, 0.3, 0.5, 0.7, and 0.9]. The experimental parameters are listed in Table 9 and the results are shown in Figure 13. They provide a clear and compelling illustration of how network quality acts as a critical control parameter for system security.

Table 9. Parameters for controlled convergence analysis of network coefficient w .

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	30	10	20	10	15	0.1	$x^* = x_2 = 1$
300	30	10	20	10	15	0.3	$x^* = x_3 = 0.5$
300	30	10	20	10	15	0.5	$x^* = x_1 = 0$
300	30	10	20	10	15	0.7	$x^* = x_1 = 0$
300	30	10	20	10	15	0.9	$x^* = x_1 = 0$

The experimental results align with our theoretical predictions across all three equilibrium cases. As shown in Figure 13a, when the network quality is poor ($w = 0.1$), the illicit gain from attacking is minimal. The system unequivocally converges to the all-honest equilibrium ($x^* = 1$), regardless of the initial proportion of honest miners. The convergence process takes approximately 0.6 s. Figure 13b demonstrates the tipping point. At a medium network quality of $w = 0.3$, the incentives for attacking and remaining honest are balanced. The system stabilizes at a mixed strategy equilibrium $x^* = 0.5$, precisely as predicted by formula $x_3 = (c_1 + c_2 + a - wnd)/a$. This state represents a fragile balance where opportunistic attacks persist within the population. Notably, the convergence to this mixed state is the slowest among the tested scenarios, taking around 0.8 s. As depicted in Figure 13c–e, once w crosses a profitability threshold (at $w > 0.4$), the all-attack strategy ($x^* = 0$) becomes the sole stable equilibrium. These figures clearly show a trend that when w increases from 0.5 to 0.9, the system converges to this harmful state much more quickly.

At $w = 0.9$, the system collapses to the all-attack state in less than 0.1 s, highlighting the intense economic pressure to attack when network conditions are favorable.

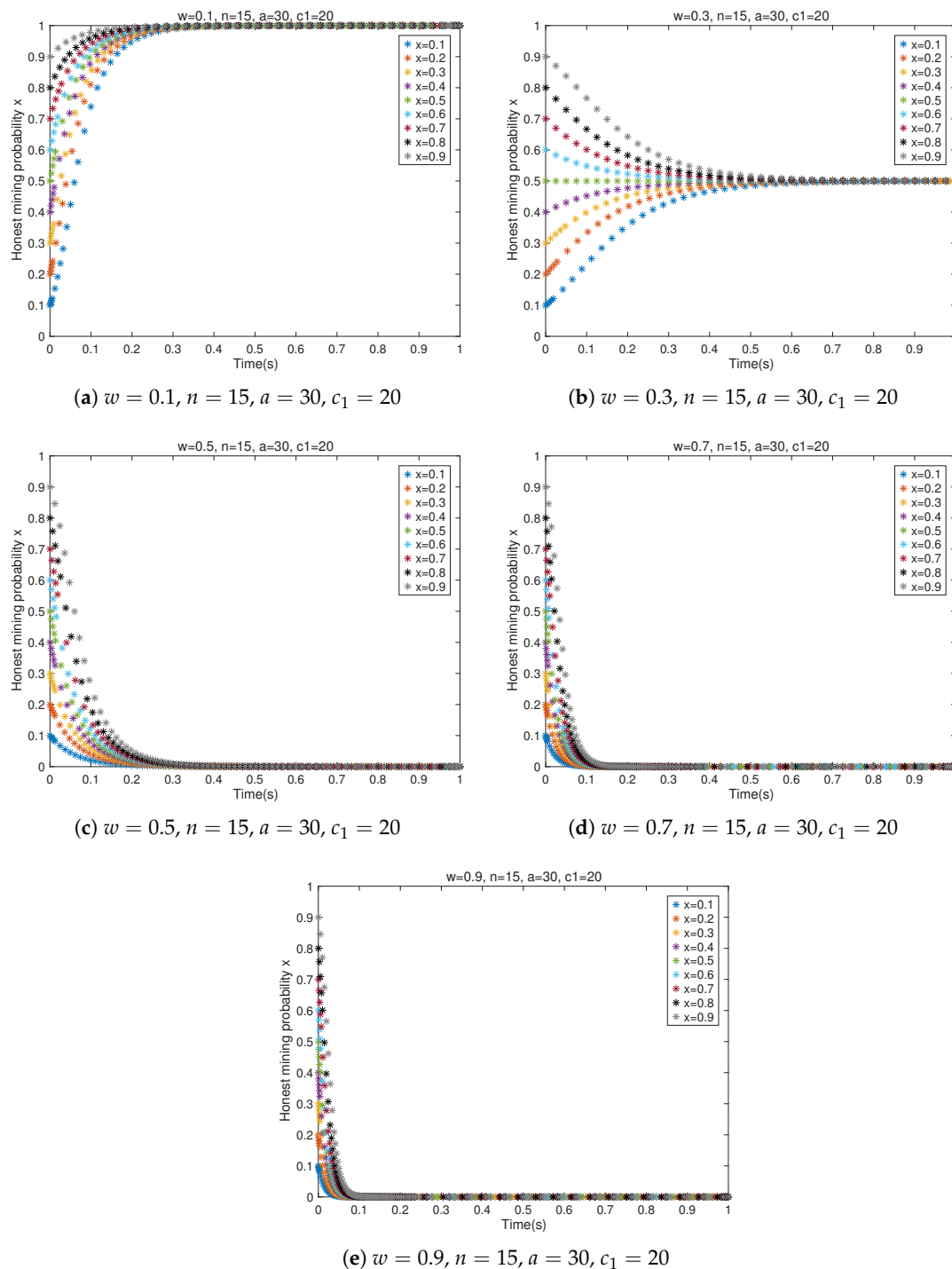


Figure 13. Convergence performance under varying network environment coefficient w .

A key finding is that improving network quality paradoxically increases DDoS attack incentives, thereby degrading system security. This occurs because better network conditions make attacks more effective and profitable. To address this, system designers must implement adaptive mechanisms where penalty c_1 and reward a are automatically adjusted as network conditions change.

6. Discussion

Discussion 1: The model assumes two mining pools with equal computational power. What are the limitations of this assumption? How would hashrate heterogeneity change the equilibrium structure and convergence trajectories?

Answer: Equal hashrate is just a simplifying assumption that enables tractable analysis. But it ignores that varying cost-benefit trade-offs lead pools of different sizes to adopt distinct strategies. And it masks the strategic advantage of scale, where dominant pools can absorb attack costs that smaller pools cannot, resulting in fundamentally different equilibria. In practice, mining pools have heterogeneous computational power, which alters game structure. With unequal hashrates, the symmetric replicator dynamics become asymmetric. Specifically, the payoff matrix depends on the hashrate ratio, changing the one-dimensional dynamics $F(x) = dx/dt$ into multi-dimensional dynamics. Consequently, the original equilibrium condition $x_3 = (c_1 + c_2 + a - wnd)/a$ ($a > 0$) no longer applies. Each pool adopts a distinct optimal strategy based on its relative computational power. This heterogeneity also alters both the equilibrium location and the convergence trajectory. Pools with different hashrates may face different cost-benefit trade-offs, potentially leading to distinct optimal strategies. Analyzing this asymmetric case requires multi-dimensional dynamics beyond the current model.

Discussion 2: The model assumes perfect attacker identification. What limitations arise from this simplifying assumption? How would detection latency and false positives/negatives change the payoff matrix and equilibrium strategies?

Answer: The perfect attacker identification assumption simplifies the model for tractable baseline analysis but deviates from practical detection scenarios. Real detection systems face latency, false negatives (FNs), and false positives (FPs) that modify the model's payoff structure and equilibrium results. If detection is delayed by time Δt , attackers profit during this time before penalties are imposed. The effective attack gain increases from wnd to approximately $w(1 - e^{-\lambda\Delta t})nd$, where λ represents detection sensitivity. This shifts the equilibrium toward more aggressive strategies. An FN means missed attacks escape penalty c_1 , dropping the expected penalty to $c_1(1 - p_{fn})$, where p_{fn} denote the false negative rate. The new equilibrium becomes $x'_3 = [c_1(1 - p_{fn}) + c_2 + a - wnd(1 + p_{fn})]/a$, lowering x_3 to further incentivize attacks. An FP wrongly penalizes honest pools, reducing their reward to $a(1 - p_{fp})$ and discouraging honest mining, where p_{fp} denote the false positive rate. Ultimately, imperfect detection systematically shifts equilibrium toward attack-dominant strategies and reduces convergence to honest mining.

Discussion 3: The model assumes no miner migration. What are the limitations of this assumption? If miners can freely migrate between pools, would the equilibrium strategy distribution change, or only the convergence speed?

Answer: The absence of miner migration is a simplifying assumption that restricts the model's practical fidelity. The static fixed-hashrate setup fails to capture miners' actual hash reallocation across pools. And miner migration has two fundamentally different effects depending on its mechanism. If miners only change strategies while pool hashrates remain fixed, the equilibrium x^* stays the same but convergence speeds up. If miners reallocate hashrate, the equilibrium fundamentally changes. When miners migrate, the hashrate distribution $n(t)$ changes over time. The equilibrium condition becomes time dependent: $x_3(t) = [c_1 + c_2 + a - w \cdot n(t) \cdot d]/a$. This couples strategy dynamics with hashrate dynamics, creating a two-dimensional system. The equilibrium x is no longer stationary; it drifts as $n(t)$ evolves. In practice, modeling miner migration properly requires coupled strategy-hashrate dynamics and more sophisticated frameworks (mean-field games, differential games). This is beyond the scope of the current work but represents an essential future direction.

Discussion 4: The model treats attack cost c_2 as constant, independent of attack scale. How would a cost function $c_2(n) = kn$ affect parameter sensitivity results?

Answer: The current model assumes c_2 is fixed, representing the base overhead of launching any attack. This is appropriate when analyzing strategic pool responses rather than attack deployment economics. However, in scenarios where attack cost scales with the number of malicious nodes, a linear cost function $c_2(n) = kn$ becomes more realistic. This would change the equilibrium to $x'_3 = (c_1 + kn + a - wnd)/a$. It alters parameter sensitivity, especially for n . The net effect of increasing n depends on whether the marginal attack gain wnd exceeds the marginal attack cost k . With fixed c_2 , higher n increases attack incentives as wnd dominates. With $c_2(n) = kn$, the cost kn opposes the gain wnd , creating a trade-off where the optimal n balances marginal gains and costs. The effects of c_1 and a remain qualitatively similar but change in magnitude due to this trade-off.

Discussion 5: The model treats network environment coefficient w as common knowledge. In reality, attackers may falsely signal poor network conditions while exploiting good networks for attacks. How does information asymmetry affect results?

Answer: Information asymmetry fundamentally undermines our baseline model. In such scenarios, mining pools form distorted beliefs about the true w and converge to a wrong equilibrium $x'_3 = \frac{c_1 + c_2 + a - w_{\text{claimed}}nd}{a}$ instead of the true x_3 . Meanwhile, attackers gain asymmetric deception profits, defined as $\Delta\pi = (w_{\text{true}} - w_{\text{claimed}})nd$. To address this, future work can incorporate incomplete information Bayesian games and signaling frameworks, in which mining pools establish probabilistic beliefs $b(w)$ toward the true network state. And the game becomes: (1) Nature draws w ; (2) Attacker sends a signal σ ; (3) Pools choose strategies x based on their belief $b(w|\sigma)$.

7. Conclusions

This paper investigates the evolutionary game dynamics of mining pools within blockchain networks subjected to DDoS attacks, deriving stable strategies via replicator dynamics equations. By analyzing the influence of key parameters such as the number of attacking nodes, penalties, and rewards on strategy convergence and game sensitivity, we provide comprehensive insights into mining pool behaviors across various network environments. Experimental results based on both dynamic and static game models demonstrate that the proposed approach effectively identifies optimal strategies and captures the convergence process of mining pools. Notably, as network conditions improve, mining pools exhibit a greater propensity to adopt DDoS attack strategies for higher returns. Thus, we need to strike a balance between the optimization of network infrastructure and the fairness and security of the blockchain. However, this study only relies on simulation verification and adopts relatively idealized model assumptions. Future work will pursue three directions: (1) empirical validation against real blockchain network data and agent-based simulations with realistic attack scenarios; (2) extension to multi-pool environments with heterogeneous delays, cross-pool miner migration and attack–defense co-evolution models; (3) incorporation of imperfect information through Bayesian games to address information asymmetries and strategic deception regarding network conditions. These extensions will enhance the model’s scalability and robustness in practical blockchain ecosystems.

Author Contributions: Conceptualization, X.L. and Z.W.; methodology, X.C., X.L. and D.D.; software, Y.Z. and J.L. (MATLAB R2025a); validation, X.L., Z.W. and Z.L.; formal analysis, X.C. and D.D.; investigation, X.C., Z.L. and Y.Z.; resources, Z.L., X.C. and J.L.; data curation, X.L. and J.L.; writing—original draft preparation, X.C., Y.Z. and J.L.; writing—review and editing, X.L., Z.L. and D.D.; visualization, Z.L. and D.D.; supervision, Z.L. and Z.W.; project administration, X.L., Z.L. and Z.W.;

funding acquisition, X.L., Z.L. and Z.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Guyuan City Science and Technology Research and Development Program (2025GKJYF0006), and Henan Provincial Key Research and Development Program in Science and Technology (262102210186).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors would like to thank the anonymous reviewers for their valuable comments and constructive suggestions, which have significantly improved the quality of this manuscript. We are also grateful to Zhao Huang from Xi'an University of Posts and Telecommunications for his valuable help and continuous support throughout this research.

Conflicts of Interest: The authors declare that they have no competing interests.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
PoW	Proof of Work
DDoS	Distributed Denial-of-Service
DEG	Dynamic Evolutionary Game
ESS	Evolutionary Stable State
ML	Machine Learning
BWH	Block Withholding
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance

Appendix A. Parameter Traversal and Equilibrium Validation

To enhance experimental robustness and remedy the limited parameter settings in the main text, this appendix presents extensive parameter traversal results under typical network environment coefficients, covering harsh, medium, and good network scenarios.

Appendix A.1. Parameter Traversal Under Harsh Network Condition

This section evaluates the model equilibrium strategies under a harsh network environment with $w = 0.2$.

Table A1. Parameter traversal results under harsh network condition, $w = 0.2$.

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	30	10	15	10	20	0.2	$x^* = x_3 = 0.5$
300	30	10	35	10	20	0.2	$x^* = x_2 = 1$
300	30	10	15	10	30	0.2	$x^* = x_1 = 0$

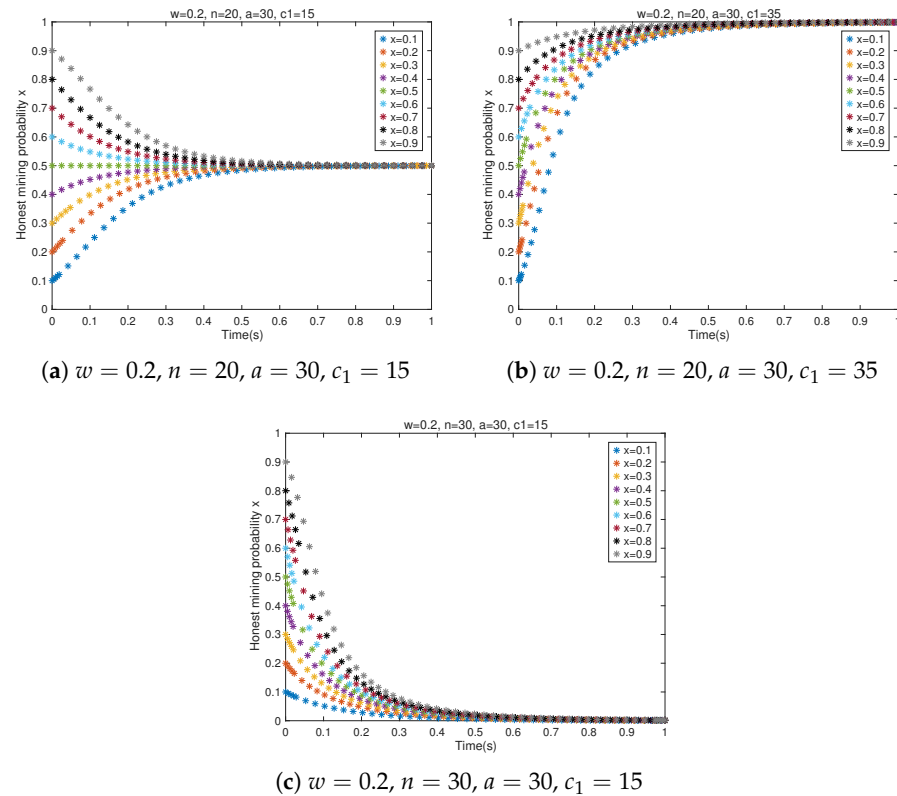


Figure A1. Game convergence experiments in harsh network environments.

Appendix A.2. Parameter Traversal under Medium Network Condition

This section evaluates the model equilibrium strategies under a medium network environment with $w = 0.4$.

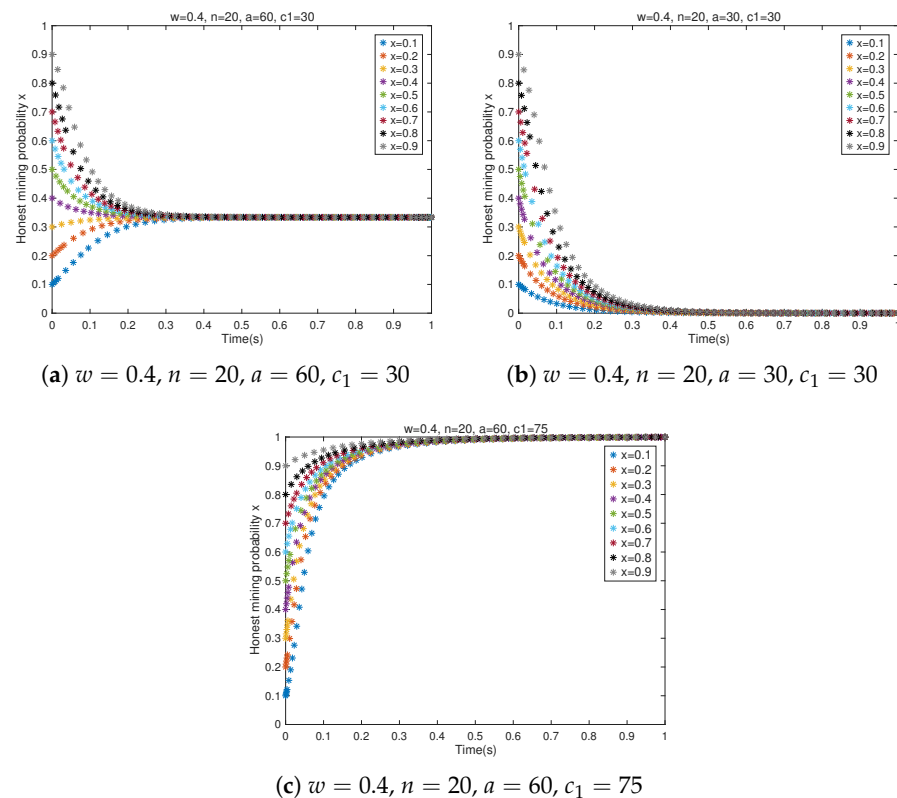


Figure A2. Game convergence experiments in medium network environments.

Table A2. Parameter traversal results under medium network condition, $w = 0.4$.

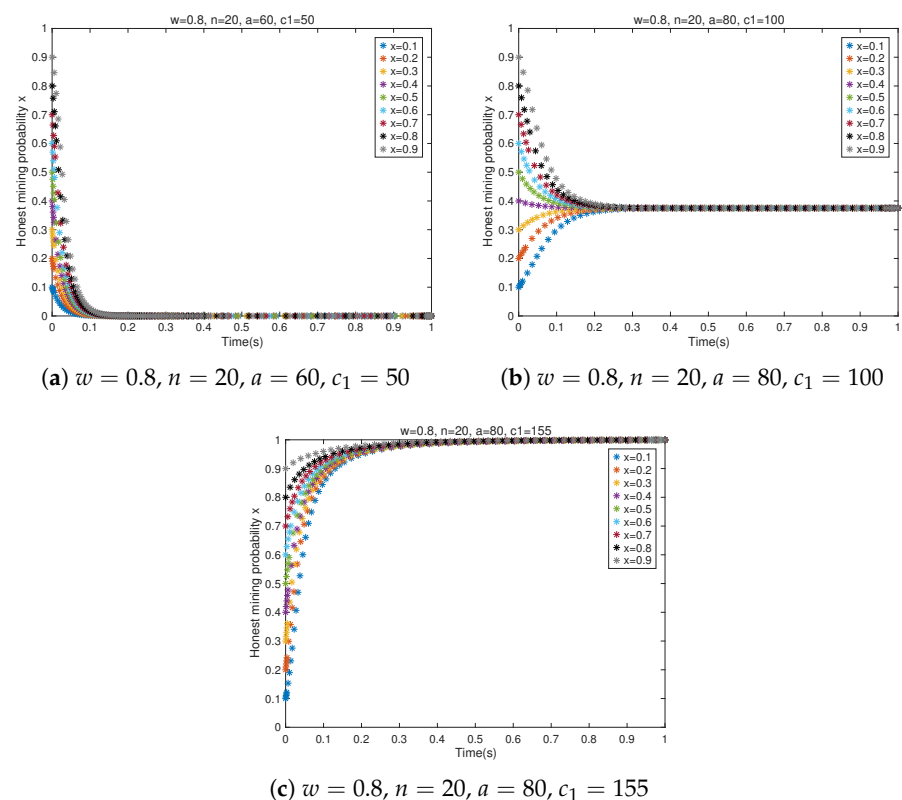
Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	60	10	30	10	20	0.4	$x^* = x_3 = 0.33$
300	30	10	30	10	20	0.4	$x^* = x_1 = 0$
300	60	10	75	10	20	0.4	$x^* = x_2 = 1$

Appendix A.3. Parameter Traversal Under Good Network Condition

This section evaluates the model equilibrium strategies under a good network environment with $w = 0.8$.

Table A3. Parameter traversal results under good network condition, $w = 0.8$.

Profits R	Rewards a	DDoS Gains d	Penalty c_1	Attack Cost c_2	Pools Controlled n	Net Env. w	Optimal Strategy x^*
300	60	10	50	10	20	0.8	$x^* = x_1 = 0$
300	80	10	100	10	20	0.8	$x^* = x_3 = 0.375$
300	80	10	155	10	20	0.8	$x^* = x_2 = 1$

**Figure A3.** Game convergence experiments in good network environments.

References

1. Nugraha, R.; Rendragra, A.D.; Shin, S.Y. Integrated electric ground vehicle and drone with blockchain-driven routing delivery. *Comput. Oper. Res.* **2025**, *180*, 105057. [CrossRef]
2. Lakhan, A.; Mohammed, M.A.; Al-Badawi, L.Q.; Memon, S.; Slan, V.; Deveci, M.; Martinek, R. Enhancing efficiency in blockchain harvest: Empowering transparent trading in agricultural applications. *Alex. Eng. J.* **2025**, *118*, 91–104. [CrossRef]
3. Aldawsari, H. A blockchain-based approach for secure energy-efficient IoT-based wireless sensor networks in smart cities. *Alex. Eng. J.* **2025**, *126*, 1–7. [CrossRef]

4. Sun, P.J.; Wan, Y.; Wu, Z.D.; Fang, Z.X.; Li, Q. A survey on privacy and security issues of IoT-based environments: Technologies, protection measures, and future directions. *Comput. Secur.* **2025**, *148*, 105097. [\[CrossRef\]](#)
5. Chaganti, R.; Bhushan, B.; Ravi, V. The role of blockchain in DDoS attacks mitigation: Techniques, open challenges and future directions. *arXiv* **2022**, arXiv:2202.03617.
6. Hayat, R.F.; Aurangzeb, S.; Aleem, M.; Srivastava, G.; Lin, J.C.W. ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments. *IEEE Trans. Eng. Manag.* **2022**, *71*, 12605–12618.
7. Wang, Q.H.; Xia, T.Y.; Wang, D.; Ren, Y.Z.; Miao, G.X.; Choo, K.K.R. SDoS: Selfish mining-based denial-of-service attack. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 3333–3349. [\[CrossRef\]](#)
8. Zhang, Y.; Gai, K.K.; Zhu, L.H.; Qiu, M.K. An auxiliary classifier GAN-based DDoS defense solution for blockchain-defined industrial networks. In Proceedings of the International Conference on Smart Computing and Communication, New York, NY, USA, 18–20 November 2022; pp. 319–328.
9. Nkoom, M.; Hounsinnou, S.G.; Crosby, G.V. Securing the internet of robotic things against DDoS attacks: A federated learning with differential clustering approach. *Comput. Secur.* **2025**, *155*, 105493. [\[CrossRef\]](#)
10. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of blockchain for mitigating distributed denial-of-service attacks. *Secur. Priv.* **2020**, *3*, e96.
11. Venkatesan, K.; Rahayu, S.B. Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques. *Sci. Rep.* **2024**, *14*, 1149. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Benkhaddra, I.; Kumar, A.; Setitra, M.A.; Bensalem, Z.E.A.; Lei, H. Prevention of DDoS attacks using optimized deep learning approach in blockchain technology. *Trans. Emerg. Telecommun. Technol.* **2023**, *34*, e4729. [\[CrossRef\]](#)
13. Katib, I.; Ragab, M. Blockchain-assisted hybrid harris hawks optimization based deep DDoS attack detection in IoT environment. *Mathematics* **2023**, *11*, 1887. [\[CrossRef\]](#)
14. He, Q.; Wang, C.; Cui, G.M.; Li, B.; Zhou, R.; Zhou, Q.G.; Xiang, Y.; Jin, H.; Yang, Y. A game-theoretical approach for mitigating edge DDoS attack. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 2333–2348. [\[CrossRef\]](#)
15. Gupta, M.; Kumar, R.; Shekhar, S.; Sharma, B.; Patel, R.B.; Jain, S.; Ben Dhaou, I.; Iwendi, C. Game theory-based authentication framework to secure internet of vehicles with blockchain. *Sensors* **2022**, *22*, 5119. [\[CrossRef\]](#) [\[PubMed\]](#)
16. 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, Qingdao, China, 18–21 August 2023; pp. 78–83.
17. Liu, X.; Huang, Z.; Wang, Q.; Jiang, X.H.; Chen, Y.; Wan, B. Analyzing miners' dynamic equilibrium in blockchain networks under DDoS attacks. *Electronics* **2023**, *12*, 3903. [\[CrossRef\]](#)
18. Wang, C.H.; Chu, X.W.; Qin, Y. Dissecting mining pools of bitcoin network: Measurement, analysis and modeling. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 398–412. [\[CrossRef\]](#)
19. Xu, J.; Wang, C.; Jia, X.H. A survey of blockchain consensus protocols. *ACM Comput. Surv.* **2023**, *55*, 1–35. [\[CrossRef\]](#)
20. Yadav, A.K.; Singh, K.; Amin, A.H.; Almutairi, L.; Alsenani, T.R.; Ahmadian, A. A comparative study on consensus mechanism security threats and future scopes: Blockchain. *Comput. Commun.* **2023**, *201*, 102–115. [\[CrossRef\]](#)
21. Hameed, K.; Barika, M.; Garg, S.; Amin, M.B.; Kang, B. Taxonomy study on securing blockchain-based industrial applications. *J. Ind. Inf. Integr.* **2022**, *26*, 105312. [\[CrossRef\]](#)
22. Kabla, A.H.H.; Anbar, M.; Manickam, S.; Al-Amiedy, T.A.; Cruspe, P.B.; Al-Ani, A.K.; Karuppayah, S. Applicability of intrusion detection system on ethereum attacks: A comprehensive review. *IEEE Access* **2022**, *10*, 71632–71655. [\[CrossRef\]](#)
23. Guru, A.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A survey on consensus protocols and attacks on blockchain technology. *Appl. Sci.* **2023**, *13*, 2604. [\[CrossRef\]](#)
24. Khan, Z.A.; Namin, A.S. A survey of DDoS attack detection techniques for IoT systems using blockchain technology. *Electronics* **2022**, *11*, 3892. [\[CrossRef\]](#)
25. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [\[CrossRef\]](#)
26. Chen, Y.R.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z.P. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confid. Comput.* **2022**, *2*, 100048. [\[CrossRef\]](#)
27. Yakubu, B.M.; Khan, M.I.; Khan, A.; Jabeen, F.; Jeon, G. Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home. *Digit. Commun. Netw.* **2023**, *9*, 383–392. [\[CrossRef\]](#)
28. Shirvani, G.; Ghasemshirazi, S.; Azgomi, M.A. Mitigating DDoS attacks on the internet of things using federated learning. *Peer-Netw. Appl.* **2025**, *18*, 198. [\[CrossRef\]](#)
29. Dai, Q.Y.; Zhang, B.; Dong, S.Q. A DDoS-attack detection method oriented to the blockchain network layer. *Secur. Commun. Netw.* **2022**, *2022*, 5692820. [\[CrossRef\]](#)
30. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks. *Comput. Ind.* **2023**, *144*, 103801. [\[CrossRef\]](#)

31. Wu, S.K.; Chen, Y.J.; Li, M.H.; Luo, X.Y.; Liu, Z.; Liu, L. Survive and thrive: A stochastic game for DDoS attacks in bitcoin mining pools. *IEEE/ACM Trans. Netw.* **2020**, *28*, 874–887. [\[CrossRef\]](#)
32. Johnson, B.; Laszka, A.; Grossklags, J.; Vasek, M.; Moore, T. Game-theoretic analysis of DDoS attacks against bitcoin mining pools. In *Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 72–86.
33. Zheng, R.X.; Ying, C.W.; Shao, J.; Wei, G.Y.; Yan, H.Y.; Kong, J.M.; Ren, Y.K.; Zhang, H.; Hou, W.G. New game-theoretic analysis of DDoS attacks against bitcoin mining pools. In *Network and System Security*; Springer: Cham, Switzerland, 2019; pp. 567–580.
34. Sood, A. DDOS attacks against bitcoin mining pools. In *Proceedings of the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, Greater Noida, India, 12–13 May 2023*; pp. 2398–2402.
35. Eyal, I. The miner’s dilemma. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–20 May 2015*; pp. 89–103.
36. Chaganti, R.; Bhushan, B.; Ravi, V. A survey on blockchain solutions in DDoS attacks mitigation. *Comput. Commun.* **2023**, *197*, 96–112. [\[CrossRef\]](#)
37. Tran, M.; von Arx, T.; Vanbever, L. Routing attacks on cryptocurrency mining pools. In *Proceedings of the 2024 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–22 May 2024*; pp. 3805–3821.
38. Chen, J.M.; Cheng, Y.K.; Xu, Z.Q.; Cao, Y. Decision on block size in blockchain systems by evolutionary equilibrium analysis. *Theor. Comput. Sci.* **2023**, *942*, 93–106. [\[CrossRef\]](#)
39. Ren, N.; Li, B.Z. Research on evolutionary game and prevention strategy of blockchain 51% double spend attack. *Comput. Eng. Appl.* **2020**, *56*, 28–34.
40. Tang, C.B.; Yang, B.S.; Zhang, Y.; Lin, F.L.; Chen, G.R. Cooperation and optimization of multi-pool mining game with zero determinant alliance. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 4965–4978. [\[CrossRef\]](#)
41. Ratnayake, R.; Kliyange, M.; Murphy, L. Blockchain data trust benchmark dataset. *IEEE Data Descr.* **2025**, *2*, 296–303. [\[CrossRef\]](#)
42. Liu, X.; Huang, Z.; Wang, Q.; Wan, B. An evolutionary game theory-based method to mitigate block withholding attack in blockchain system. *Electronics* **2023**, *12*, 2808. [\[CrossRef\]](#)
43. Fujita, K.; Zhang, Y.Y.; Sasabe, M.; Kasahara, S. Mining pool selection problem in the presence of block withholding attack. In *Proceedings of the 2020 IEEE International Conference on Blockchain, Rhodes Island, Greece, 2–6 November 2020*; pp. 321–326.
44. Zhang, J.X.; Wu, M. Cooperation mechanism in blockchain by evolutionary game theory. *Complexity* **2021**, *2021*, 1258730. [\[CrossRef\]](#)
45. Wang, F.F.; Liang, N.J.; Wu, F.G.; Zhou, B.; Nie, J.W.; Zhang, X. Three-party evolutionary game-based analysis and stability enhancement of improved PBFT consensus mechanism. *Clust. Comput.* **2024**, *27*, 1–27. [\[CrossRef\]](#)
46. Sun, J.X.; Zhao, R.; Yin, H.R.; Cai, W. Incentive mechanism for redactable blockchain governance: An evolutionary game approach. *IEEE Trans. Comput. Soc. Syst.* **2024**, *11*, 6953–6965. [\[CrossRef\]](#)
47. Samuelson, L. Evolution and game theory. *J. Econ. Perspect.* **2002**, *16*, 47–66. [\[CrossRef\]](#)
48. Strogatz, S.H. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*; CRC Press: Boca Raton, FL, USA, 2015.
49. Maynard Smith, J. *Evolution and the Theory of Games*; Cambridge University Press: Cambridge, UK, 1982.
50. Tatarenko, T.; Kamgarpour, M. Payoff-based learning of nash equilibria in merely monotone games. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 1790–1799. [\[CrossRef\]](#)
51. Abbasi, M.H.; Arjmandzadeh, Z.; Zhang, J.F.; Krovi, V.; Xu, B.; Mishra, D.K. A coupled game theory and lyapunov optimization approach to electric vehicle charging at fast charging stations. *IEEE Trans. Veh. Technol.* **2024**, *73*, 14224–14235. [\[CrossRef\]](#)
52. Li, H.Y.; Huang, W.H.; Duan, Z.J.; Mguni, D.H.; Shao, K.; Wang, J.; Deng, X.T. A survey on algorithms for nash equilibria in finite normal-form games. *Comput. Sci. Rev.* **2024**, *51*, 100613. [\[CrossRef\]](#)

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.