electronics

Article

An Evolutionary Game Theory-Based Method to Mitigate Block Withholding Attack in Blockchain System

Xiao Liu, Zhao Huang *, Quan Wang and Bo Wan

School of Computer Science and Technology, Xidian University, Xi'an 710071, China; cantona@stu.xidian.edu.cn (X.L.); qwang@xidian.edu.cn (Q.W.); wanbo@xidian.edu.cn (B.W.)
* Correspondence: z_huang@xidian.edu.cn; Tel.:+86-1879-261-0378

Abstract: Consensus algorithms are the essential components of blockchain systems. They guarantee the blockchain's fault tolerance and security. The Proof of Work (PoW) consensus algorithm is one of the most widely used consensus algorithms in blockchain systems, using computational puzzles to enable mining pools to compete for block rewards. However, this excessive competition for computational power will bring security threats to blockchain systems. A block withholding (BWH) attack is one of the most critical security threats blockchain systems face. A BWH attack obtains the reward of illegal block extraction by replacing full proof with partial mining proof. However, the current research on the BWH game could be more extensive, considering the problem from the perspective of a static game, and it needs an optimal strategy that dynamically reflects the mining pool for multiple games. Therefore, to solve the above problems, this paper uses the method of the evolutionary game to design a time-varying dynamic game model through the degree of system supervision and punishment. Based on establishing the game model, we use the method of replicating dynamic equations to analyze and find the optimal strategy for mining pool profits under different BWH attacks. The experimental results demonstrate that the mining pools will choose honest mining for the best profit over time under severe punishment and high supervision. On the contrary, if the blockchain system is supervised with a low penalty, the mining pools will eventually choose to launch BWH attacks against each other to obtain the optimal mining reward. These experimental results also prove the validity and correctness of our model and solution.

Keywords: PoW consensus algorithm; BWH attacks; evolutionary game theory; mining pools

check for updates

Citation: 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. https://doi.org/10.3390/electronics12132808

Academic Editor: Paris Kitsos

Received: 19 May 2023
Revised: 8 June 2023
Accepted: 13 June 2023
Published: 25 June 2023

Copyright: © 2023 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 digital economy is a concept with a broad connotation. It is an economic form that uses data to guide resources to play a role and to promote the development of productive forces [1]. As an essential part of the digital economy, a blockchain system is a decentralized byzantine consensus distributed system with tamper-proof ledgers and good data consistency [2]. Blockchain systems are widely deployed in complex application scenarios such as finance [3], Internet of Things (IoT) [4], healthcare [5], and digital wallets with dynamically changing requirements [6]. However, blockchain systems are facing some security problems. Attackers usually use substantial computing power to create a forked chain, intercept block rewards, and forge IP addresses to obtain the rewards of the servers, such as honest mining [7]. A fork chain is when malicious nodes create redundant private chains on their computing power. When the length of the private chain is longer than the public chain of the honest node, the malicious node can keep the profits of the public chain for itself. A forge IP address attack is when malicious nodes forge the transaction address of honest nodes to obtain illegal profits. An intercept block reward attack is when malicious nodes send miners to intercept the revenue of honest mining nodes. Such attack scenarios will benefit the attackers considerably, but the victims in the blockchain systems will suffer

substantial financial losses. Therefore, it is necessary to conduct in-depth research on the security of blockchain systems.

Bitcoin is the most widely used blockchain system. It is part of a public chain of blockchain systems [8] using the PoW consensus algorithm to maintain data consistency in decentralized distributed systems [9]. The public chain faces four kinds of attacks: BWH [10], fork after block withholding (FAW) [11], selfish mining [12] and 51% computing power [12]. A BWH attack is an attack mode in which malicious nodes obtain illegal gains by satisfying partial proof of work by honest miners. A FAW attack refers to the malicious node, and it dispatches miners using part of their computing power to perform a BWH attack to obtain revenue. Then, it uses part of the mining power to create redundant private chain forks to obtain more revenue. A selfish mining attack refers to malicious nodes using their computing power to create redundant forks to obtain illegal profits. In total, a 51% computing power attack means that the malicious node occupies 51% of the absolute majority of the computing power of the whole blockchain, and the block reward mined by the honest node later belongs to the private chain where the malicious node occupies the absolute computing power. Among these attacks, BWH is the most common in the Bitcoin system. A malicious pool usually sends a portion of the miners mining below it to launch a BWH attack on the honest pool. These malicious miners disguise themselves as honest pool miners and obtain excess illegal block rewards by submitting proof of partial mining works (PPoWs) instead of proof of full mining works (FPoWs) by honest miners [13]. The research on BWH attacks can be divided into the following categories: miner attack, mining pool attack, mixed attack and BWH defense strategy [14]. In order to solve the security threat caused by a BWH attack on a blockchain system, many studies have focused on static modeling of BWH attacks on a blockchain system [15–19]. These static game methods are very effective when the number of games in the mining pool is limited. These methods mainly model the mining pools, or miners, into Nash equilibrium (NE) state and zero-determinant game theory (ZDG) [20]. The current static game methods can effectively make the mining pool obtain an optimal mining strategy in the face of a BWH attack when the number of games is limited. In general, they only focus on the game of two mining pools [21,22]. Therefore, to solve the above problems for the static game, it is necessary to establish a dynamic game model to implement the dynamic selection of the mining pool and its optimal profit mining strategy.

This paper proposes an evolutionary game approach to mitigate a BWH attack. We analyze the BWH attacks problem that two mining pools need to establish a dynamic game model, and we provide the modeling and assumptions for their problem. Then, we establish the corresponding average income equation and the dynamic replication equation. According to the blockchain system's punishment degree and strict supervision, we can obtain different optimal mining strategies for mining pools. We also analyze which strategy the mining pool must choose to obtain the best reward under different BWH attack scenarios effectively. Finally, we use the zeros function from Matlab to establish the dynamic replication equation and the ode45 function to solve the dynamic replication equation, conduct three experiments and obtain the optimal stable policy solution under different degrees of supervision and punishment. In summary, we make the following novel contributions:

- To the best of our knowledge, this paper is the first to use a dynamic method to study the selection of the profitable optimal strategy for mining pools under a BWH attack.
- Based on the change in the supervision and punishment degree of the blockchain system, this paper implements a model in which mining pools with different probabilities can smoothly be used to select the optimal strategy of obtaining block rewards under different BWH attack scenarios over time using the evolutionary game method.
- We obtain optimal strategies regarding the different degrees of punishment and the tightness of regulation in a blockchain system by analyzing various BWH attack situations on the dynamic replication equation.

- The experimental results show that a dynamic evolutionary game can effectively make the mining pool select the optimal strategy to obtain a block reward under different parameter transformations and BWH attack scenarios of the blockchain system. The experimental results also show that the model and solving method can satisfy the defect that the profit status of static game players cannot change with time.

The structure of this paper is as follows. Section 2 provides information on a blockchain, PoW, Evolutionary game theory, and BWH attacks. In Section 3, in the face of a BWH attack, we describe the proposed mining pools model and the optimal strategy solutions in different situations based on evolutionary game theory. In Section 4, we evaluate the effectiveness of our solution against BWH attacks based on two mining pools. Section 5 concludes the paper.

2. Background

2.1. Blockchain System

Blockchain is a chain data structure that sequentially combines data blocks following chronological order. It is a distributed ledger that cannot be tampered with or forged and secured by cryptography. Because of the decentralization and immutability of blockchain, many fields, such as finance and IoT, have begun to establish their blockchain systems according to application requirements. As Figure 1 below shows, a blockchain system typically consists of six layers: a data layer, a network layer, a consensus layer, an incentive layer, a contract layer, and an application layer [23]. The most critical layer in the blockchain system is the consensus layer. The consensus layer in the blockchain mainly ensures that the data in the node ledger are not tampered with and upholds data consistency.

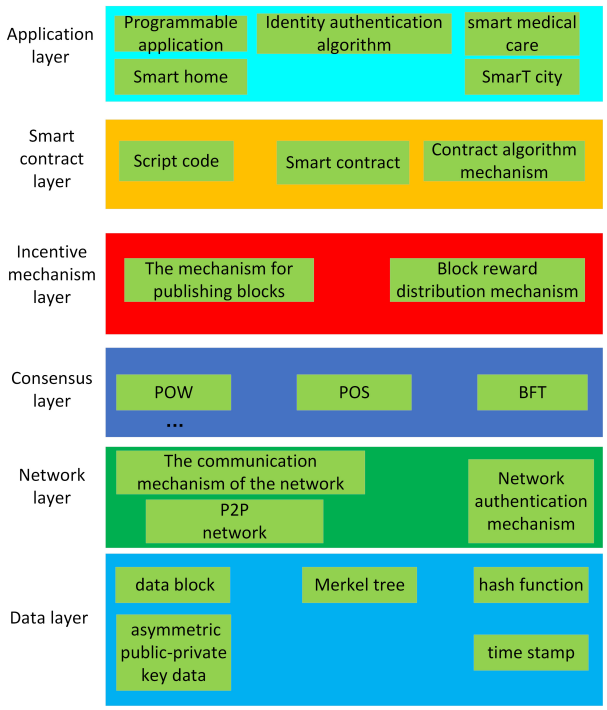


Figure 1. The composition of the blockchain system architecture.

The fundamental core of the consensus layer is composed of consensus algorithms. Consensus algorithms are a broad class of algorithms that find applications in many fields. Consensus algorithms can be widely used in many applications related to blockchain systems, such as wireless sensor networks, machine learning, swarm robotics, etc. [24–27]. There are various kinds of consensus algorithms. According to different application requirements, the corresponding consensus algorithms are adopted to ensure the data consistency, fault tolerance, and security of the whole blockchain system [27]. Presently, some analy-

ses on consensus algorithms are in more than just distributed systems and blockchains. The research on these consensus algorithms extends to wireless sensor networks, machine learning, and other fields. Moussa et al. [24] proposed using a formal software engineering technique, statistical model checking, to model and assess the robustness of consensus-based behaviors from a communication standpoint in robot collaboration. Bondugula et al. [25] proposed a novel weighted consensus model to minimize the number of false negatives and false positives without compromising accuracy. Kenyeres et al. [26] proposed a distributed mechanism to detect whether a graph was bipartite regular and identified how to reconsider the algorithm so that the convergence of the average consensus algorithm was guaranteed over regular bipartite graphs. The mainstream consensus algorithms include PoW, PoS, and Raft. The PoW algorithm can effectively ensure the data consistency of the public chain in the decentralized blockchain system [27], which is also the focus of this paper.

2.2. Pow Consensus Algorithm

The PoW consensus algorithm is one of the most commonly utilized consensus algorithms in blockchain systems [28]. The essence of the PoW algorithm is the mining process, which uses an incentive mechanism to make mining pools and miners compete with each other to mine new blocks. The PoW consensus algorithm process is mainly composed of three parts: mining process [28,29], incentive mechanism [30,31] and key verification [32,33]. The specific application scenario process using the PoW algorithm is shown in Figure 2 below. In this scenario, the mining process consists of two steps: user notification and mining pool competition. Identity key authentication consists of identity authentication and the blockchain system adding new blocks. Therefore, the scenario of the PoW consensus algorithm mainly consists of six parts. From Figure 2, we can see that the PoW algorithm requires multiple miners to compete to mine in the same mining pool. The pool manager uses an incentive mechanism to motivate miners to compete through higher computing power. When the block has been mined, the pool manager uses the identity authentication algorithm to verify the security and correctness of the mined block. Then, the pool manager adds the block to the blockchain. Through the study [28–33] of these three parts, we concluded that the PoW algorithm contains the following advantages. First, the PoW algorithm process is a simple way to ensure the high performance and scalability of the blockchain system through simple mining and decentralized structure. Secondly, the PoW algorithm can effectively use incentive and authentication mechanisms to prevent mining attacks on malicious nodes. Due to its mining process and decentralized nature, the PoW algorithm is often used in the applications such as cryptocurrency, IoT, innovative healthcare, and Smart city [33,34].

However, the application scenarios above focused on the mining process. The fierce competition among mining nodes can bring security risks to the blockchain system. In the mining process, the PoW consensus algorithm mainly obtains block reward through mining pools competing with each other under these application scenarios. Multiple mining pools competing with each other will consume a lot of power and bring insecurity to the blockchain system. Malicious nodes usually use more substantial computing power to create redundant private chain forks (selfish mining attacks) or forge IP addresses (sybil attacks) to obtain block rewards from honest mining pools (BWH attacks). This situation will bring great economic losses and security threats to the blockchain system. Based on these situations, numerous studies [27,35] on the issues of PoW security have produced research on the security of the PoW consensus algorithm. A BWH attack is one of the most common security threats to a blockchain system in the mining process under these applications, and it is also the main issue to focus on in this paper.

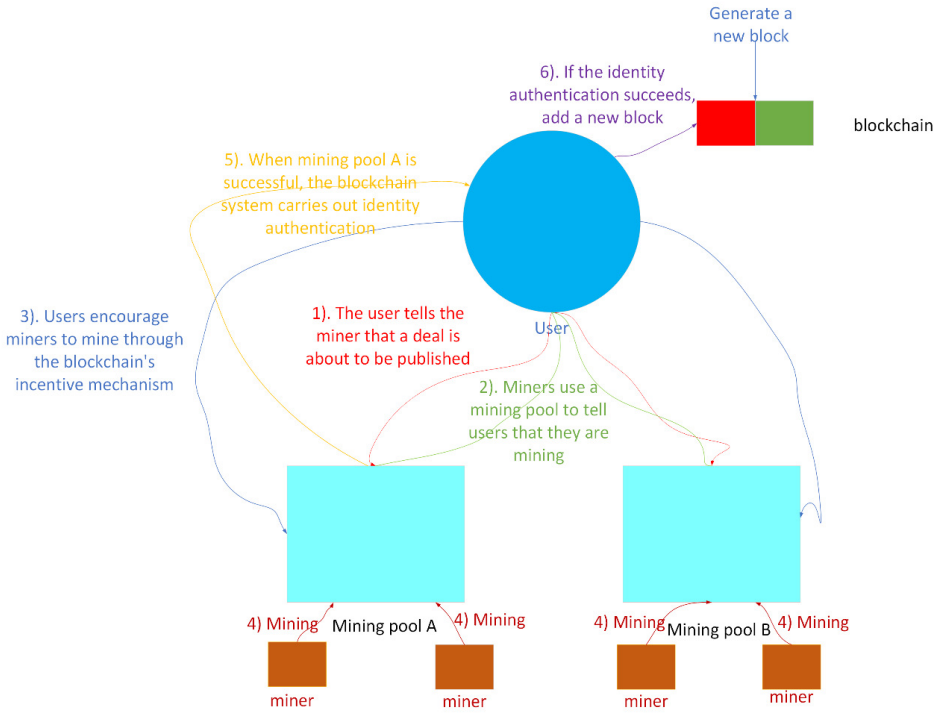


Figure 2. Diagram of PoW algorithm.

2.3. Block Withholding Attack

A BWH attack is a part of the primary attacks the PoW algorithm faces. The essence of a BWH attack on the PoW algorithm is that malicious nodes sacrifice part of their computing power to carry out attacks to replace the proof of honest node mining to obtain illegal block production rewards. Multiple malicious nodes can perform BWH attacks on the same honest mining node simultaneously or at different times to obtain profits. The occurrence of this situation will cause more loss to the honest node. However, this attack situation often occurs when more than two mining pools are modeled. One scenario of a BWH attack is shown in Figure 3 below. From Figure 3, we can analyze a BWH attack process as follows. First, a blockchain system has two mining pools which are used to obtain the block rewards. Second, when multiple miners work for a mining pool, they must submit a certificate of employment to demonstrate that they work honestly. Third, the malicious node only submitted PPoWs instead of a miner's FPoWs to obtain mining profits [35]. This means that the malicious miners only submit part of the answers to the pool administrator by discarding all the successful answers, leading to the loss of the mining pools. Finally, the malicious pool obtains an illegal block reward. Honest mining pools suffered economic losses. Therefore, when the attacker in the block system launches a BWH attack using the PoW algorithm, the mining rewards of other mining pools will be significantly reduced.

Malicious mining pools in the blockchain system launch BWH attacks to obtain illegal block production rewards. This behavior brings substantial economic losses to honest mining pools. However, the reward of mining pools launching BWH attacks against each other will be lower than that of honest mining. This is the mining dilemma between the mining pools under BWH attacks [35]. Therefore, determining how to use the means of the dynamic game to resist BWH attacks and solve the mining dilemma is the main challenge that we face.

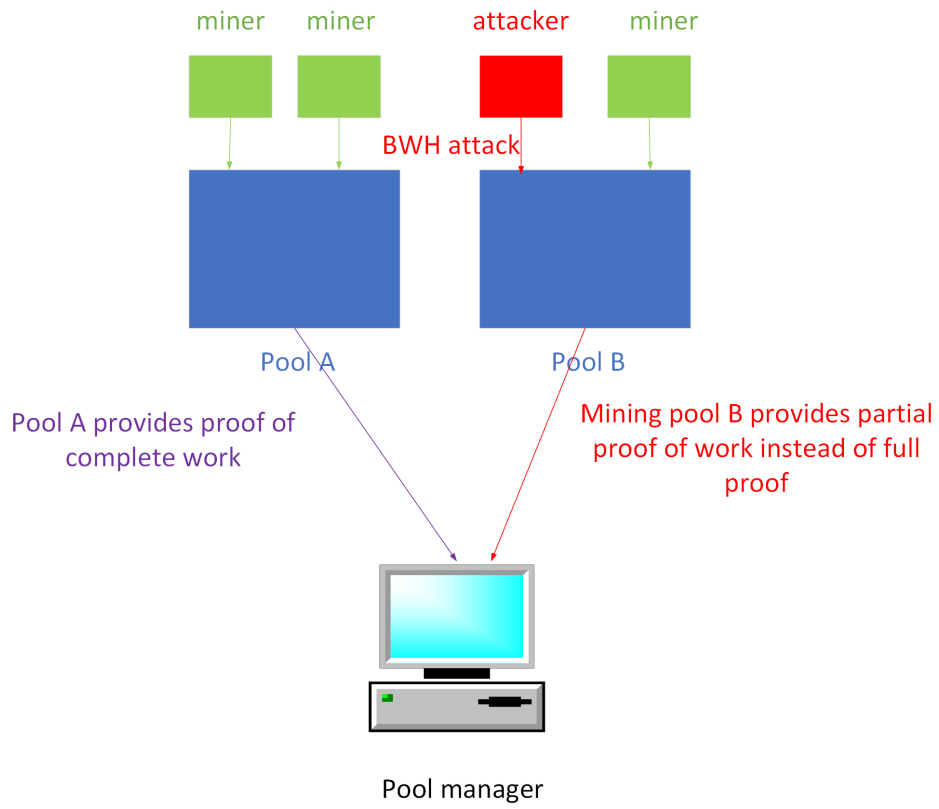


Figure 3. A scenario of mining pool facing BWH attack under blockchain system.

2.4. Research Progress And Related Work

Since a BWH attack was proposed, it has been attracting the attention of researchers. Solving this problem can effectively maintain the data security of the PoW consensus algorithm and ensure the regular operation of the blockchain system [35,36]. The BWH attacks research is mainly conducted using the game theory method. The blockchain system uses the game and reinforcement learning method to make the mining pool choose the strategy with the optimal rewards given to the mining pool by the blockchain system. This strategy generates new blocks when facing a BWH attack, which can minimize the loss caused by a BWH attack. Mining pools compete for computing power to generate new blocks. The block reward will be allocated to the mining pool that mines the block honestly. The attacker launches a BWH attack on the honest mining pool to obtain the block reward. There is no straightforward relationship between the blocks and a BWH attack. Blocks cannot observe the occurrence of BWH attacks. The attacking mining pool launching BWH attacks maximizes its interests to obtain the block reward for the honest pool. Therefore, using a strategy that reduces the loss of the honest mining pool under a BWH attack is necessary. The academic researchers studying BWH attacks mainly adopt the methods of game theory and reinforcement learning so that the mining pool chooses the mining strategy with the maximum profit and rewards in the blockchain system. The current research on a BWH attack work is divided into two parts: how the mining pool models the profit optimal in the face of attacks and how miners select the profit optimal of the mining pool. The first study examines how to model the mining pool to obtain the optimal profit when the mining pool is faced with a BWH attack. A BWH attack scenario studied in the former category is assumed to contain only mining pools without miners. The second type of research mainly studies how miners choose different mining pools to obtain optimal profits, assuming that both miners and mining pools exist [36].

Numerous kinds of research focus on analyzing and addressing how miners choose mining pools to obtain optimal profits when facing BWH attacks. Fujita et al. [37] applied reinforcement learning (RL) techniques to analyze the optimal pool selection of miners.

This work effectively addressed the issue of the mining pool's strategy to attract more miners to obtain the optimal block reward when the two mining pools face a BWH attack. Fujita et al. [38] modeled the pool selection process of miners in the two pools as an evolutionary game and found the Evolutionarily Stable States (ESSs) of the game as the solutions to take full advantage of the profits of the miners. Chen et al. [39] proposed a prevention method of block withholding attack (PMBWA) based on miners' mining behavior in a blockchain to prevent the block withholding attack. Kim et al. [40] proposed an evolutionary game model and solution based on the miners who confronted BHW attacks in multiple mining pools to choose which mining pool had the best profit.

Some researchers focus on obtaining the optimal strategy for mining pools facing BWH attacks. Can et al. [41] proposed a conceptual framework for analyzing reward-sharing schemes in two mining pools when confronting the BHW attacks. Tuo et al. [42] designed a novel model built by the evolutionary game theory to analyze the BWH attacks in multiple mining pools. Wang et al. [43] implemented a game analysis strategy for multiple mining pools facing BWH attacks. This method ensured that the mining pool could get the most out of its response strategy when the pool received a sharp decrease in profits from attacks. Ren et al. [44] proposed to apply zero-determinant strategies to optimize the behavior selection of the mining pool under the PoW consensus mechanism to increase the aggregate revenues of the system.

However, there are two defects in the current research on BWH attacks. First, these works mainly focus on the problem of how miners dynamically select a mining pool to obtain the optimal profit when a BWH attack has been conducted between the mining pools. This research on BWH attacks' penetration profit of mining pools ignores the profit consideration of selecting the optimal strategy profit for the mining pool itself. Second, the contemporary research on the two pools mainly focuses on the profit analysis of miners in the pools when the pools are facing a BWH attack. There is no in-depth research on the reward analysis of mining pools in the face of the BWH attacks. Even if researchers were aware of this problem, most of these studies use dynamic game methods to solve the problem of which mining pool miners choose the optimal reward when mining pool attacks occur. These studies [41,42] ignore the research on the optimal strategy selection when the mining pool faces a BWH attack.

Therefore, to deal with these problems, the works of this paper are described below:

1. This paper proposes an evolutionary game model based on the profit of two mining pools.

2. We solve the steady state by replicating the dynamic equation and analyzing the mining pool's optimal profit strategy under different circumstances through the system penalty degree and supervision coefficient.

3. Experiments have demonstrated that this model utilizes the dynamic game method to effectively obtain the optimal mining strategy for the mining pool.

The experimental results show that our model can provide a virtual environment for the mining pool dilemma problem where only honest mining is the optimal strategy.

3. The Proposed Evolutionary Game Theory Model and Solutions

3.1. Problem Description

BWH attacks damage the benefits of honest mining pools. Attackers profit from being attacked. Suppose the blockchain system can regulate the punishment and profit of the mining pool. In that case, the mining pool can effectively choose the corresponding strategy to earn the best profits through the game strategy. In this paper, we examine the issue of BWH attacks between the two mining pools. Parameters and symbols appearing in modeling and solutions in this paper are given in Table 1 below.

Table 1. BWH attack modeling parameter table for mining pools.

Parameters	Description and Function of Parameters
R	Mining pool revenue from honest mining.
d	The illegal revenue gained by the attacker or the revenue lost by the attacked mining pool.
a	The blockchain system gives rewards to honest mining pools and punishments to attacking mining pools.
k	The supervision coefficient of blockchain system on launching BWH attack mining pool.
w_1	The average return of honest mining by a mining pool.
w_2	Average return of a mining pool launching a BWH attack.
$\overline{w}$	Average return of a mining pool.
$F(x)$	The dynamic equation of replication for x and time t.
$F'(x)$	The first derivative of $F(x)$ with respect to the probability x of honest mining.
x	The probability that the pool mines honestly.
$x_i(i = 1, 2, 3 \dots)$	The different steady states computed by the replicated dynamic equation.
x^*	Deterministic mining strategies under different degrees of punishment and supervision.

The two pools have equal computational power. This paper does not consider the infiltration of miners between the pools and the re-selection of the pools. Major attack scenarios refer to the literature [45]. Table 1 describes the parameters required to establish the BWH attack game model.

(1) The blockchain system we are considering is run on a public chain using the PoW Consensus algorithm. The system is facing a BWH attack.

(2) The blockchain system has two mining pools, A and B. Both pool A and B have the same initial computational power. The number of miners in each pool is stable. Miners in one pool cannot decide to go to another pool to mine the blocks.

(3) When all the pools are mined honestly, they make a reward of R. The range of values for R is $R > 0$.

(4) Suppose that when one pool mines honestly but the other pool attacks. The blockchain system gives mining pools that mine honestly a certain degree of reward, which is set as a. The blockchain system that gives the penalty for the pool which launches the BWH attack is also set to a. The attacker attacks an honest mining pool. The loss of the honest mining pool is set as d. The profits of the mining pool launching the BWH attack are also d. The value of a is $a \geq 0$. Likewise, the value of d is $d \geq 0$. $a = 0$ means that the reward or punishment of the blockchain system to the mining pool is 0, which means that the pool is honestly mining. $d = 0$ means that no mining pool in the blockchain system launches a BWH attack, and the loss d suffered by the attacked mining pool is 0.

(5) The blockchain system provides a certain degree of supervision for the mining pools that launch BWH attacks, and the supervision coefficient is set as k. We assume that there is a penalty from the blockchain system for launching an attack on the mining pool. The blockchain system gives the attacking pool a ka degree of punishment. The range of k stands at $0 < k < 1$. The larger the value of k, the greater the supervision degree of the blockchain system for the mining pool.

(6) Since A and B have the same computational power, the two mining pools launch attacks to gain profits from each other. Therefore, both launch BWH attacks against each other to obtain illegal gains and losses are d.

(7) The modeling in this paper does not consider the cost of launching BWH attacks in mining pools. Parameters changed in this paper include the supervision coefficient k and the punishment intensity of the blockchain system on mining pools a. The mining pool profits R from honest mining, and the loss and gain d from launching the attack are fixed values.

3.2. ESS Model Description

This paper mainly refers to [40,45] modeling for a BWH attack. In the study of this paper, the main part of the research involves two pools with the same computational power faced with a BWH attack, for which the mining pool will choose to obtain the best strategy. This paper assumes that the blockchain system has two mining pools A and B. Then, if a BWH attack occurs in the blockchain system, we will conduct a detailed analysis. There are four attack situations in the blockchain system. In other words, we divide the mining pool attack into the following four categories: A and B are honest mining, A attacks B, B attacks A, and A and B attack each other. In this paper, we call the practice of mining pools *Mining Honest*, H for short. Therefore, we identify the following four attack situations, namely $(H, H), (H, BW), (BW, H), (BW, BW)$. (H, H) means that pool A and pool B mine honestly. (H, BW) means that mining pool A mines honestly and mining pool B launches a BWH attack to mining pool A. (BW, H) means that mining pool B mines honestly and mining pool A launches a BWH attack to mining pool B. (BW, BW) means that pool A and pool B launch BWH attacks against each other. We define the left side of each row as whether pool A attacks and the right side as pool B's behavior. The following is an analysis of the benefits of mining pool A and B under each of the four attack scenarios.

(1) For the first BWH attacks situation, namely (H, H), both pool A and B are honest in mining and get rewards. According to the definition of Section 3.1 above, the profit obtained from honest mining in the A mining pool is R, and the rewards from the pool B is R. The BWH attack in the first case is shown in Figure 4.



Figure 4. Both pools A and B are honest mining.

(2) The second case is about the attack of the mining pool (H, BW). This attack case implies that, in this case, pool A mines honestly, and pool B launches a BWH attack. Pool B is rewarded with a certain amount of illegal blocking through BWH attacks, which is set as d. The blockchain system gives pool A a particular reward to pool A for honest mining, which is set as a. Mining pool B launches a BWH attack, and the blockchain system gives a certain degree of punishment, which is set as ka. Pool A and pool B receive a block production reward of R when mining at full capacity. So, the reward for pool A in this situation is $R - d + a$. The profit from pool B is $R + d - ka$. The BWH attack in the second case is illustrated in Figure 5.

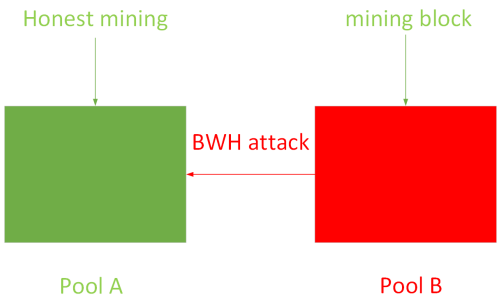


Figure 5. Pool B launches a BWH attack on pool A.

(3) The third case is about the attack of the mining pool (BW, H). In this case, mining pool A launches a BWH attack on mining pool B, while pool B is honest mining. Pool A attacks pool B to obtain a portion of the illegal block reward from B, which is set to d. B loses d's block production reward. Due to the attack launched by mining pool A, the blockchain system punishes pool A at the degree of ka. The blockchain system regulates the mining pool A through the regulation coefficient k. Pool B is honest in mining, and the blockchain system rewards B with the degree of a. Pool A and pool B receive a block production reward of R when mining honestly in a blockchain system. Therefore, in this case, the value of pool A's profits is $R + d - ka$. The rewards obtained by B are $R - d + a$. The BWH attack in the second case is shown in Figure 6.

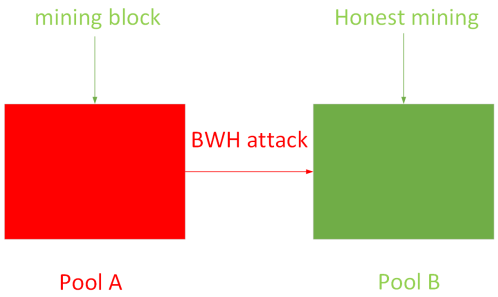


Figure 6. Pool A launches a BWH attack on pool B.

(4) The fourth case is about the attack of the mining pool (BW, BW). In this case, pool A and B launch BWH attacks against each other. All the mining pools are no longer mining honestly. Mining pool A launches a BWH attack to obtain the forbidden block reward d from mining pool B. At the same time, A also tackles the loss of degree d caused by the BWH attack from mining pool B. Therefore, the block generation reward for pool A interacting with pool B is 0. Because of a BWH attack on mining pool A, the blockchain system gives pool A punishment of degree ka. For Pool A, the profit of honest mining is R. Therefore, the profit of pool A in this situation amounts to $R - ka$. In the case of mining pools launching BWH attacks against each other, the profit of mining pool B amounts to the same as that of mining pool A, and the reward of the pool B amounts to $R - ka$. The BWH attacks, in this case, are illustrated in Figure 7.

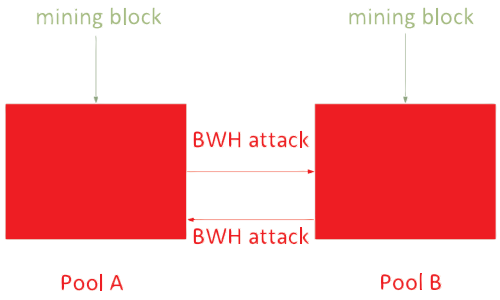


Figure 7. Pool A and B launch BWH attacks against each other.

Based on the above parameters' description and the establishment of the BWH attack model of two mining pools, we can establish and describe each mining pool's profit game theory table under different attack conditions. Then, the game theory income table of the mining pool A and B under four attacks is shown as follows. Table 2 describes the rewards for pool A and pool B under the four different BWH attacks. The horizontal table indicates whether mining pool B launches a BWH attack or honest mining, and the vertical table indicates whether mining pool A launches a BWH attack. H for honest mining, BW for a BWH attack. The (R, R) symbols in Table 2 relate to the payoffs of pool A and B under different attack scenarios. The former is the reward of pool A under different BWH attacks, while the latter represents the reward of pool B.

Table 2. The reward of Pool A and Pool B when it is attacked by BWH.

Pool A \ Pool B	**H**	**BW**
H	(R, R)	$(R - d + a, R + d - ka)$
BW	$(R + d - ka, R - d + a)$	$(R - ka, R - ka)$

Each element in Table 2 represents Pool A's payoff when Pool A and Pool B exhibit honest mining (H) or attack (BW). Table 2 shows that the rewards of mining pool A and mining pool B are the same when they face different BWH attack situations. The rewards of mining pool A and pool B have to conform with the form of a typical two-agent symmetric game. Then, this game situation is an evolutionary game with symmetric same game agents. We only need to create the replication dynamics equation for the four attack cases to determine whether BWH attacks one of the mining pools A or B and obtain a stable solution to obtain all stable strategies.

After the reward situation of each mining pool has been obtained, we use the procedure of an evolutionary game to solve the different solutions of replication dynamics. We should solve all possible strategies that mining pools may choose when facing BWH attacks by solving the method of replicating dynamic equations. These strategic solutions in the evolutionary game model refer to different solution number values of the honest mining probability of the mining pool. We presume that when the mining process has started, the probability of honest mining selected by the mining pool is x. The probability of attack selected for the mining pools is $1 - x$. The range of the honest mining probability of the mining pool x is $0 \leq x \leq 1$.

From Table 2, we can conclude that the average value of reward w_1 of honest mining pool mining for the mining pool is as follows. w_1 represents the revenue of the initial mining pool with the expected reward obtained with the honest mining strategy.

$$w_1 = x * R + (1 - x) * (R - d + a). \tag{1}$$

Similarly, we can use w_2 to represent the expected value of the reward that the mining pool launches a BWH attack.

$$w_2 = x * (R - ka + d) + (1 - x) * (R - ka). \tag{2}$$

So from Equations (1) and (2), we can conclude that the expected return of the mining pool is $\overline{w}$. The expected reward $\overline{w}$ is described by Equation (3) below.

$$\begin{aligned} \overline{w} &= x * w_1 + (1 - x) * w_2 \\ &= x * [x * R + (1 - x) * (R - d + a)] + (1 - x) * [x * (R - ka + d) + (1 - x) * (R - ka)] \\ &= x^2 * R + x(1 - x) * \{[(2R + (1 - k) * a)]\} + (1 - x)^2 * (R - ka) \end{aligned} \tag{3}$$

We solve the different strategy solutions that the mining pool game may choose through the replication dynamic equation method of evolutionary game theory combined with the average revenue $\overline{w}$ when the mining pool faces a BWH attack. The approach used to obtain the changed strategy of the evolutionary game model of this paper is to solve the dynamic replication equation for x in the time t dimension. This paper solves the possible, stable states of the replication dynamics according to the Lyapunov method [42] and the evolutionary game-solving strategy of reference [46,47]. Then, the dynamic replication equation $F(x)$ implemented in this paper is included as Equation (4).

$$\begin{aligned} F(x) &= dx(t)/dt \\ &= x(w_1 - \overline{w}) \\ &= x[(1-x)w_1 - (1-x) * w_2] \\ &= x(1-x)(w_1 - w_2) \\ &= x(1-x)[x * R + (1-x) * (R - d + a) - x * (R - ka + d) - (1-x) * (R - ka)] \\ &= x(1-x)[(ka-d)x + (a + ka - d)(1-x)] \\ &= x(1-x)(a + ka - d - ax) \end{aligned} \tag{4}$$

We set the value of the dynamic replication equation $F(x)$ equal to 0, and thus we can obtain the evolutionary game's three possible state solution values.

$$\begin{aligned} F(x) &= 0 \\ x(1-x)[a + ka - d - ax] &= 0 \end{aligned} \tag{5}$$

We can obtain three stable states by solving the dynamic replication equation. The three solutions of the dynamic replication equation, which set the x_i $(i = 1, 2, 3 \dots)$ as representations, are broken down as indicated in Equation (6) below. The value of x_i can occur in the following two cases.

(1) If x_i is a deterministic probability value such as 0 or 1, then the range of x_i is $0 \leq x_i \leq 1$.

(2) When x_i is not a definite probability value but a variable expression containing varying parameter values, the penalty force a and the supervision coefficient k, then the value range of x_i is the whole set of real numbers, namely $x_i \in R$. R is the entire set of real numbers. If the value of x_i is $x_i < 0$ or $x_i > 1$, then this x_i is not in the final stable solution. According to the uncertain value of x_i in this situation, we need to divide the cases to discuss and obtain a stable solution in the final different cases.

$$x_1 = 0, x_2 = 1, x_3 = \frac{a + ka - d}{a} \tag{6}$$

Among these possible stable solutions, the values of x_1 and x_2 are determined to be 0 and 1, respectively. This means there are two possible stable strategies for solving the model in this paper: solution x_1 and solution x_2. However, we cannot determine under what supervision and punishment intensity the corresponding stable strategy can be obtained. The solution to this problem must rely on the uncertain policy solution x_3. However, the solution to the steady state x_3 is undefined, and we need to compare it with the values of x_1 and x_2 to discuss the case by case. As the value of x_3 is uncertain, penalty intensity a and supervision coefficient k will change. In the next section, we must discuss the value of x_3 by six cases to determine the value range of the value of penalty intensity a and k. In our discussion of a and k, neither a nor k is equivalent to 0. $a = 0$ means that the blockchain system has no penalty or reward for the pool to remain in the original honest mining state. $k = 0$ means there is no blockchain supervision for launching attacks on mining pools, which does not meet the practical requirements. After we obtain the values of a and k, we use the method in literature [47] to solve the stable solution of the evolutionary game model under different conditions. The first derivative of $F(x)$ to x is $F'(x)$. The $x_i(i = 1, 2, 3 \dots)$ value satisfying $F'(x) < 0$ is a stable strategy solution in the case of an exact attack. Finally, we need to obtain the slope image of $F'(x)$ by discussing the value of x_3 in different attack cases to obtain the final stable solution.

3.3. Steady State Solutions

After solving the steady state of the mining pool in the blockchain system, a detailed analysis of the steady state under different degree publishing a and Supervision coefficient k is required. The blockchain determines which strategy is the best profit for the mining pool with different initial values through different values of a and k. Different cases of k and

a allow a blockchain system to determine the optimal mining strategy for the mining pool under various attack scenarios. We classify the uncertain solution x_3 in the evolutionary game model. This section discusses x_3 by comparing the size relationship of x_1 to x_2. At the same time, we change the range of a and k and divide the whole x_3 into six cases. We can determine the most profitable strategy for the mining pool under different circumstances. This paper analyzes the value of steady-state x_3 for the three steady states of Equation (6) and discusses the selection of mining pool strategy under the three conditions of $x_3 \leq 0$, $0 < x_3 < 1$ and $x_3 \geq 1$.

(1). **When $x_3 \leq 0$ occurs; that is to say,** $\frac{a+ka-d}{a} \leq 0$.

Since x is the probability of honest mining in the mining pool, the value of x should meet the requirement that $x \geq 0$. In this case, we solve for the stable solution x^*, depending on the different values of a and k; that is, the value of x^* that satisfies $F'(x^*) < 0$. So, the steady-state value that fits this situation is $x_1 = 0$, $x_2 = 1$. There should be two cases in which $x_3 \leq 0$, and the two cases are described below. Built on the phase diagram of replication dynamics, the solution of the unique steady-state strategy in evolutionary games must carry out certain conditions. This stable strategy solution means that only the unique stable strategy x is satisfied by the intersection of the tangent slope at the intersection of the replication dynamics equation $F(x)$ and the abscission with negative slope [41]. In other words, the x_i $(i = 1, 2, 3 \dots)$ value satisfying $F'(x) < 0$ is a stable strategy solution in the case of an exact attack. We use x^* to represent the stable mining strategy chosen by the mining pool in each case.

case A: $x_3 \leq 0$ **and** $a > 0$.

In the case of A, we focus on the value of x_3, namely $x_3 \leq 0$. When $0 < x < 1$, the value of $f(x)$ is $f(x) < 0$. In this case, the phase diagram of the dynamic replication equation about x is presented in Figure 8 below. As indicated in Figure 8, $F'(x)$ means that the slope of the intersection of $F(x)$ curve and the abscissa is negative. So, the intersection of this x-coordinate is the only steady-state solution we want to find in the case of A. We can see from Figure 8 that the mining pools' only steady state value is $x^* = 0$. In the case of A, pool A and B all choose the strategy to launch BWH attacks against each other to maximize profit.

We need to analyze the value range of the penalty strength A and the regulation coefficient k under Case A. In this case, we must determine how to take the values of a and k to make the optimal profit of the mining pools. In the case of A, we have the premise that $\frac{a+ka-d}{a} \leq 0$. Since $a > 0$, we can derive that $a + ka - d \leq 0$. Therefore, we can conclude from the above derivation and assumption that the value range of a is $0 < a \leq \frac{d}{1+k}$. The value of k will vary with the value of a. The range of k is $k \leq \frac{d-a}{a} (d > a)$. Therefore, in the case of A, the blockchain system has a low degree of punishment or reward for the mining pool and a low degree of supervision for the mining pool. Under this restriction condition, when the mining pool launches a BWH attack, all the mining pools attack each other for the best reward.

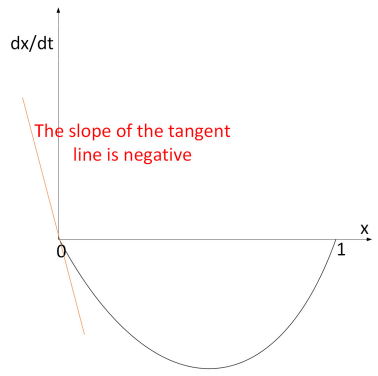


Figure 8. Phase diagram of the replicated dynamic equation in case A.

case B: $x_3 \leq 0$ **and** $a < 0$.

Because a represents the reward the system gives to the honest pool and the penalty for attacking the pool, the value of a is generally greater than 0. In this case, our assumption is $a < 0$, contrary to the previous condition that a meets $a > 0$. Therefore, this assumption does not meet the requirements of the actual blockchain system, so there is no unique steady-state strategy x^*.

(2). **When** $x_3 \geq 1$ **occurs; that is to say,** $\frac{a+ka-d}{a} \geq 1$.

In this situation, the steady-state value that fits this situation is x_1, x_2, x_3. The two cases should be described below, where $x_3 \geq 1$. We solve for the stable mining solution x^* in this attack case depending on the different values of a and k; that is, the value of x^* that satisfies $F'(x^*) < 0$.

case C: $x_3 \geq 1$ **and** $a > 0$.

In the case of C, we are focused on the value of x_3, namely $x_3 \geq 1$. This also means that $\frac{a+ka-d}{a} \geq 1$. Since $x_3 \geq 1$, $F(x)$ should always be greater than 0 when $x \in [0, 1]$. Then, the replicated dynamic phase diagram in case C is shown in Figure 9 below. The phase diagram of the replicated dynamic state shows that $F'(x) < 0$ means $F(x)$ intersects with the x-coordinate, where the slope is negative, and the state point is $x = 1$. Therefore, in the case of C, the only steady-state strategy obtained by the mining pool facing a BWH attack is $x^* = 1$. $x^* = 1$ means that all mining pools are honest in mining. Therefore, when facing a BWH attack in the blockchain system in case C, the mining pools choose the strategy of honest mining without launching BWH attacks to gain the best reward.

This paper analyzes the degree of supervision k and punishment a of a blockchain system. $\frac{a+ka-d}{a} \geq 1$ means $a + ka - d \geq a$. Therefore, it can be deduced that the value of a, in this case, is $a \geq \frac{d}{k}$. From the range of a, we can deduce that the value of k is $k \geq \frac{d}{a}$. Therefore, we can conclude from the punishment degree a and the supervision strength k. In the case of C, the blockchain system requires relatively strict supervision of the mining pool and strong punishment for block reward so that the mining pools with different initial probabilities will finally choose honest mining for the best profit over time.

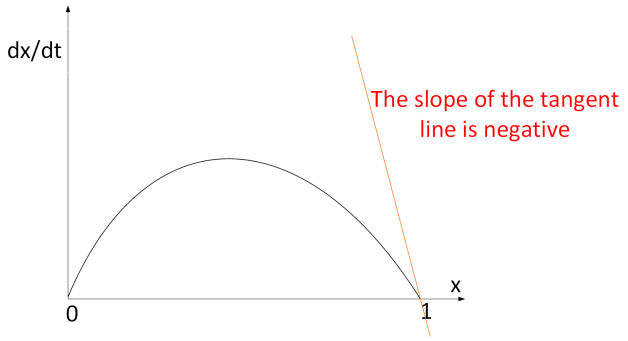


Figure 9. Phase diagram of the replicated dynamic equation in case C.

case D: $x_3 \geq 1$ **and** $a < 0$.

As in case B, our assumption is $a < 0$, contrary to the previous condition that a meets $a > 0$ in the premise of the range of a values of the game model in this paper. The assumptions in case D do not match the reality. In this case, we need help locating a stable strategy. Therefore, the assumption in case D does not meet the requirements of the existing blockchain system, so there is no unique steady-state strategy x^*.

(3). **When** $0 < x_3 < 1$ **occurs; that is to say,** $0 < \frac{a+ka-d}{a} < 1$.

In this situation, the steady-state value that fits this situation is x_3. This means that $0 < \frac{a+ka-d}{a} < 1$. We have to find the stable solution x^*. The solution satisfying $F'(x^*) < 0$ is the stable solution in this attack case. This situation falls into two cases according to the different value ranges of a. In this situation, $F(x)$ has $x_1 = 0$, $x_2 = 1$, and $x_3 = \frac{a+ka-d}{a}$ solutions that satisfy our hypothesis. However, we need to find a stable attack strategy

satisfying the hypothesis under different conditions in the three steady states by the two case discussions. Two different stable solutions are described in detail as follows.

case E: $0 < x_3 < 1$ **and** $a > 0$.

Because we find out our hypothesis that $F(x) \geq 0$ if $x \in [0, x_3]$. The value range of $F(x)$ in $x \in [x_3, 1]$ is $F(x) \leq 0$. Therefore, the replicated dynamic phase diagram of $F(x)$ in the case of E is shown in Figure 10 below. It is obvious that the slope of $F(x)$ that intersects the x-coordinate is negative only when $x = x_3$. $F'(x) < 0$ is $x = x_3$. This means that the steady-state strategy of this case is $x^* = x_3 = \frac{a+ka-d}{a}$. This steady-state solution means that the mining pools will have a certain probability of choosing to mine honestly and to launch a BWH attack, a probability-based mixed game strategy in evolutionary game theory. Therefore, when the blockchain system is faced with BWH attacks in case E, the mining pool chooses a mixed strategy to obtain the best reward by mining with a certain probability x_3.

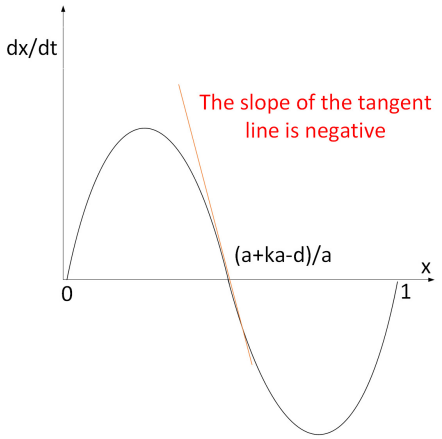


Figure 10. Phase diagram of the replicated dynamic equation in case E.

We analyze the range of punishment intensity a and supervision coefficient k in case E. $0 < \frac{a+ka-d}{a} < 1$ means $a + ka - d > 0$ and $a + ka - d < a$. $a + ka - d > 0$ means that $a > \frac{d}{1+k}$. $a + ka - d < a$ means that $a < \frac{d}{k}$. Therefore, the value range of punishment intensity a is solved as $\frac{d}{1+k} < a < \frac{d}{k}$. Using the same method and from the range of values of a, we can calculate that the value range of supervision intensity k is $\frac{d-a}{a} < k < \frac{d}{a} (d > a)$. From the above range of punishment intensity a and supervision coefficient k, we can analyze that the values of a and k are within range in this case. This means that under case E, the punishment a and supervision degree k are at a medium level when mining pools face BWH attacks. Therefore, the mining pool with different initial probability mining under the moderate degree of punishment and the degree of supervision will choose the mixed mining strategy with probability x_3 as the best profit over time.

case F: $0 < x_3 < 1$ **and** $a < 0$.

Our basic value range of the penalty degree a of the blockchain system for the mining pool is $a > 0$. The assumption $a < 0$ for a in Case F is not consistent with the value range of a in this paper. Therefore, when BWH attack occurs in case F, there is no steady state strategy in the mining pool.

4. Evaluation Results

In this section, The detailed description and performance analysis of the experiment is as follows. First, the scheme set out in the present in this paper is introduced in detail by setting the punishment degree a and supervision intensity k of the three situations. Second, we describe the experimental setup needed to select the optimal strategy in the face of a BWH attack in a blockchain system. Finally, we analyze the strategy selection of the mining pool in detail through the experimental results.

4.1. Evolutionary Stability Strategy of Mining Pools

After completing the modeling and steady-state solution of the mining pool, we need to analyze the corresponding evolutionary strategy x^* by combining the penalty intensity a and supervision coefficient k in each case. Section 3.1 of this paper above shows that the profit R from honest mining and the illegal profit d from launching a BWH attack on the mining pool are the fixed values. This paper sets the values of R and d as $R = 140$ and $d = 40$. The analysis results of evolutionary game strategies under different circumstances are presented in Table 3 below. According to the three situations of supervision and punishment in Table 3, we can smoothly evaluate the actual parameters. Table 3 lays a good foundation for us to model and solve BWH attacks through experiments. It also provides a reference for us to set specific values of different supervision frequency k and punishment intensity a parameters according to different situations.

Table 3. Evolutionary stability strategy of mining pools under BWH attack.

Degree of Punishment a	Blockchain System Supervision Coefficient k	Evolutionary Steady-State Strategy x^*	Analysis
$0 < a \leq \frac{d}{1+k}$	$0 < k \leq \frac{d-a}{a}$	$x^* = 0$	Low degree of punishment and frequency of supervision
$a \geq \frac{d}{k}$	$k \geq \frac{d}{a}$	$x^* = 1$	High degree of punishment and frequency of supervision
$\frac{d}{1+k} < a < \frac{d}{k}$	$\frac{d-a}{a} < k < \frac{d}{a}$	$x^* = \frac{a+ka-d}{a}$	Moderate degree of punishment and frequency of supervision

As shown in Table 3 above, the design of the whole experiment primarily includes three situations with the difference of supervision frequency k and punishment degree a. So, the values of k and a will change under different experimental cases. For low punishment intensity and low supervision frequency, we set the values of a and k as $a = 20$ and $k = 0.3$, respectively. In the case of moderate punishment and supervision frequency, we set the values of a and k as $a = 40$ and $k = 0.5$, respectively. For a relatively high degree of punishment and supervision frequency, we set the values of a and k as $a = 50$ and $k = 0.9$, respectively. After selecting the parameter values for the experiment, we experimented according to the parameters of the three cases. The evolution selection of the mining pool strategy obtained by the experiment should be equivalent to the value of x^* in the three cases in Table 3.

4.2. Experimental Results and Analyses

The hardware platform used in this paper is based on a laptop with a Windows 11 system, 16g memory, and Intel an i7 10870h CPU configuration. This paper, Matlab 2022b, models and solves the evolutionary game when the mining pool faces a BWH attack under a blockchain system. We set the horizontal coordinate to time t and the unit scale value of time to 0.1 s. We set the honest mining probability x as the ordinate, and the unit scale value is also 0.1. The probability x of different mining pools choosing honest mining increases from 0.1 to 0.9 to form the value of the ordinate. Based on the continuous evolution of different probability x with time t under different supervision coefficients and punishment mechanisms in Table 3, we analyze which strategy should be chosen for the mining pool. The following content elaborates on and analyzes the experimental results through the performance diagram. Through the subsequent three experiments, the mining pool attack strategies in three scenarios are analyzed and implemented. The specific numerical experiment results of the three experimental parameters are shown in Table 4 below.

Table 4. Comparison table of specific parameters and values corresponding to the three experiments.

Mining Pool Honest Mining Profit R	Illegal Profits of Mining Pools Launching BWH Attacks d	Degree of Punishment a	Supervision Coefficient k	Evolutionary Steady-State Strategy x^*	Analysis
$R = 140$	$d = 40$	$a = 20$	$k = 0.3$	$x^* = x_1 = 0$	The solution obtained in experiment a corresponds to case A in Section 3.3
$R = 140$	$d = 40$	$a = 40$	$k = 0.5$	$x^* = x_3 = \frac{a+ka-d}{a} = (40 + 0.5 * 40 - 40)/40 = 0.5$	The solution obtained in experiment b corresponds to case E in Section 3.3
$R = 140$	$d = 40$	$a = 50$	$k = 0.9$	$x^* = x_2 = 1$	The solution obtained in experiment c corresponds to case C in Section 3.3

The three experiments are assigned and solved depending on Table 4 above. As can be seen from Table 4, we need to divide the experiment into three parts according to different values of supervision coefficient k and punishment intensity a. The corresponding results of the x^* are generated according to Section 3.3 by assigning specific parameters. In the following section, we conduct three experiments to verify the stable solution x^* obtained in Tables 4 and Section 3.3.

4.2.1. Mining Pool Strategy Selection under Low Penalty and Low Supervision

The global invariant from the preceding is $R = 140, d = 40$. The system's punishment is $a = 20$, and the supervision frequency is $k = 0.3$. In this case, when the blockchain system faces a BWH attack, the optimal profit strategy choice x^* of the mining pool changes with time t, as shown in Figure 11.

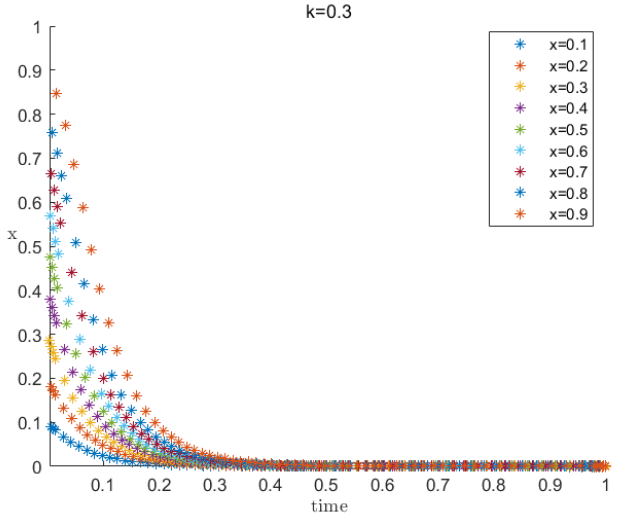


Figure 11. Under low punishment and supervision, the mining pool faces the strategy of making the best reward with time t by a BWH attack.

From Figure 11, we can put forward the following analysis of the mining pool selection. When $k = 0.3$ and $a = 20$, the blockchain system in this case has a low frequency of supervision and a low degree of punishment for all mining pools. The dashed lines with different colors are the initial honest mining of the mining pool according to different probabilities. We set the different colored dashed lines as the different honest mining probabilities x. The dashed line with $x = 0.1$ indicates that the initial honest mining probability of the pool is 0.1. With the change and progression of time, the dotted line with $x = 0.1$ converges at $time = 0.2$ s. This shows that in the case of low punishment and low regulation, the mining pools with a probability of 0.1 honest mining finally launch BWH attacks against each other to obtain the best profits. The other colored dotted lines from $x = 0.2$ to $x = 0.9$, like the dotted line with $x = 0.1$, also represent game strategies with different honest initial probability mining over time. We can see all dotted lines converge to $x = 0$. We divide the probability x of honest mining in the two pools into nine parts from 0.1 to 0.9.

The mining pools with different initial probability values (discrete dashed line colors) will finally choose what strategy to use to obtain the best profit over time when facing a BWH attack. With the advance of time t, the mining pool with different honest mining probabilities x gradually evolves from the initial probability of self-mining to the probability $x = 0$ of honest mining. After about 0.3 s from their initial probability, the honest probability x of different initial mining has evolved to 0. In the face of a BWH attack, the mining pools with other possibilities, ultimately choose the steady-state strategy of $x^* = 0$. Under the blockchain system's low-frequency supervision and low-intensity punishment, the mining pools with different initial probabilities of honest mining will eventually choose the strategy with an honest mining probability of 0 as time t changes. In other words, the mining pools finally launch BWH attacks against each other to obtain the optimal reward. Therefore, the analysis of this experimental result corresponds to the situation in Section 3.3 and Table 4 of the game-solving case A above.

4.2.2. Mining Pool Strategy Selection under Moderate Penalty and Moderate Supervision

The blockchain system's punishment is $a = 40$, and the supervision frequency is $k = 0.5$. When the blockchain system faces a BWH attack, the mining pool's optimal profit strategy choice x^* changes with time t. The specific evolution strategy selection of the mining pool is shown in Figure 12. We will discuss the experiments in this case in detail next.

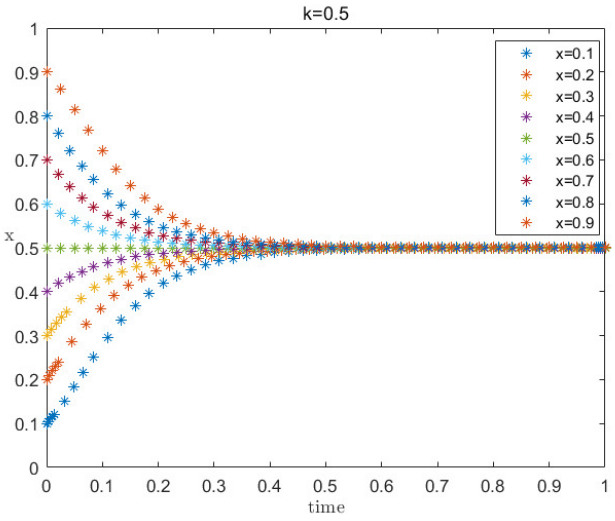


Figure 12. Under moderate punishment and supervision, the mining pool faces the strategy of making the best reward with time t by a BWH attack.

From Figure 12, we can see that the absolute probability of honest mining approaches $x = 0.5$ as time t changes for all mining pools with different mining probabilities. As in the previous experiment, other color dots represent the probability x of honest mining in different initial states of the pool. We also set separate probabilities from $x = 0.1$ to $x = 0.9$ and observe the trend over time in the medium condition of the game. Different probability values x evolve with the progression of time in the horizontal coordinate. After about 0.4 s, the chance x of all mining pools honestly approaches a stationary value $x = 0.5$. In other words, the stable strategy selected by the mining pool is $x^* = 0.5$. The blockchain system will eventually choose a mixed strategy to obtain the best profit when the mining pool faces BWH attacks under medium frequency supervision and a medium degree of punishment. In other words, the mining pools will eventually choose the strategy of honest mining probability $x = 0.5$ to obtain the best benefits. Since the degree of supervision and punishment could be more robust, the mining pools will likely launch BWH attacks to obtain benefits. The mining pool also has a certain chance of honest mining. In this case, the mixed probability strategy can only reflect the optimal strategy of mining pool profit. Therefore, the analysis of this experimental result agrees with the result of case E in Section 3.3 above.

4.2.3. Mining Pool Strategy Selection under High Penalty and High Supervision

In this case, the system's punishment is $a = 50$, and the supervision frequency is $k = 0.9$. When the blockchain system faces a BWH attack, the mining pool's optimal profit strategy choice x^* changes with time t. The precise evolution strategy selection of the mining pool is shown in Figure 13. We will discuss the experiments in this case in detail next.

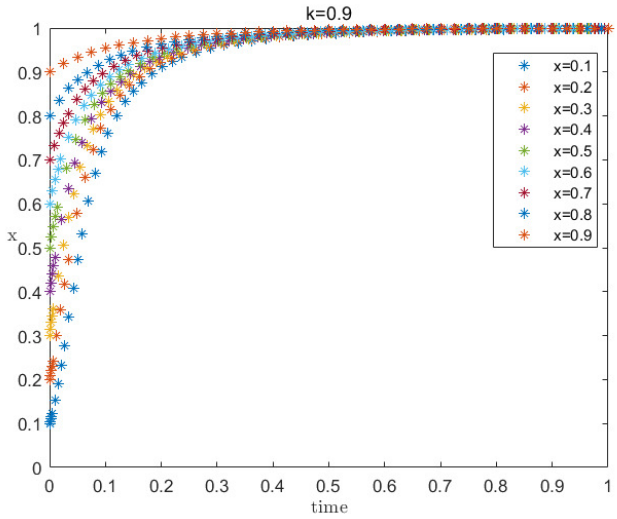


Figure 13. Under high punishment and supervision, the mining pool faces the strategy of making the best reward with time t by a BWH attack.

It can be seen from the above Figure 13 we also use dotted lines of different colors in this experiment to represent the game evolution trend of the mining pool with different honest probability mining from $x = 0.1$ to $x = 0.9$ over time. We can determine from the experimental results the probability that all the dashed lines eventually tend to be one. This means that the mining pool changes with time t and finally chooses the strategy of $x = 1$. With a time-lapse of about 0.45 to 0.5, the mining strategies selected by the pools with different mining probabilities are eventually generally consistent. In this case, the stable strategy ultimately chosen by the mining pool is $x^* = 1$. Under the blockchain system's high supervision frequency and severe punishment, the mining pool will eventually select the best reward from honest mining over time. As a result, mining pools have to consider

the high penalties and regulations of blockchain systems when launching attacks under such conditions. When a pool launches a BWH attack, its reward for its attack is smaller than the reward it receives. Therefore, all the mining pools fear the severe punishment of the blockchain system and, finally, choose the honest mining strategy. The experimental results are consistent with situation C in Section 3.3 and Table 4, indicating that our experiment is applicable and correct.

The following conclusions can be drawn from the experimental results.

(1) With the low frequency of supervision and low degree of punishment in the blockchain system, the mining pools will choose to attack each other for the best profit. Because of the low supervision of the blockchain system, the mining pool attacks are not easy to find. The mining pool easily launches BWH attacks. The blockchain system's low penalty for attacking pools means that the pools will not suffer much damage, even if they launch BWH attacks. As times goes by, the mining pool game will eventually decide to attack each other for the best profit.

(2) Under the medium supervision frequency and the medium punishment, the blockchain system will increase the supervision of the mining pool. The number of pools with varying mining rates has gradually increased in the proportion of honest mining due to increased regulation. The increased punishment of the blockchain system means that the mining pools will not earn optimal profits by mindlessly attacking each other. As time passes and evolves, some mining pools will choose to mine honestly, and others will choose to launch BWH attacks. Therefore, all pools are rewarded with the same probability of honest mining.

(3) Under the blockchain system's high supervision frequency and high punishment policy, the mining pools with different initial probabilities of mining have the best profit from honest mining over time. High regulation makes the mining pool less prone to BWH attacks. The high penalty makes the mining pool choose honest mining to avoid the loss caused by the high penalty in the dynamic game.

5. Discussion

Discussion 1: In this paper, we face that the BWH mining pool models only two mining pools, whether or assuming more than two pools are possible. Which impact would it have? Whether it is possible to assume more than two pools. Which impact would it have?

Answer: Most current research on the game theory of mining pools facing BWH attacks uses static game methods to model two mining pools [36–39]. There are expected to be very few studies on the dynamic game of the two mining pools because when the two mining pools are modeled, there are only four situations in which the mining pool launches BWH attacks that are easy to model. The attack scenario becomes very complicated if we use more than two mining pools for modeling. The number of BWH attacks in the mining pool will be more than four or even more than 10, increasing our hypothesis, description, modeling, and problem analysis. The variable parameters that affect the optimal mining strategy of BWH attack pools may include the cost of launching the attack, the number of attack pools, the penalties and rewards of the blockchain system and many more factors. At the same time, to simplify the problem when modeling, we assume that all mining pools have the same profit value. Dealing with this issue becomes more complicated when the benefits of mining pools change.

Discussion 2: The modeling solution in this paper is based on the assumptions and limitations of the model, which need to be applied in the actual application scenario. How demanding in terms of the implementation requirements is this paper's proposed approach?

Answer: There are two aspects to this discussion, and the first is how demanding our proposed approach is regarding modeling and experimental environment implementation requirements. Second, we need to discuss how demanding our model is to implement in practical applications.

First, we mainly model and analyze the mining strategies we have just started using in related work on BWH attacks. Furthermore, our current research is focused on the theoretical study of the evolutionary game of mining pools. Our dynamic evolutionary game

model chooses the attack strategy to obtain the optimal profit when two mining pools with the same computing power face BWH attacks. Our strict conditions are two mining pools with the same computing power, experimental modeling with full simulation assumption, and strict assumption modeling without considering attack cost. The environment of our experiment is to set up a model of two mining pools facing BWH attacks through Matlab software and to simulate and analyze the model.

Second, due to our stringent assumptions and full simulation, our research remains in the theoretical research stage. Numerous factors must be considered in practical applications, such as specific attack scenarios and attack costs, which will be studied in our future work. We propose to relax our modeling assumption restrictions and conduct a study of practical applications of this model using embedded clustering and PUF techniques in the next step.

6. Conclusions and Future Work

This paper proposes a mining pool game model based on BWH attacks. In this game method, an evolutionary game model is established to simulate the profit of BWH attacks in the double mining pool under the blockchain system. This paper establishes a dynamic replication equation based on the regulatory frequency and penalty intensity to obtain the optimal steady-state strategy under different decisions. The experimental results show that only when the blockchain system insists on high supervision and punishment for the mining pool will the mining pool choose the honest mining strategy to earn the best profit when faced with BWH attacks. At the same time, the experimental results demonstrate that our modeling and mathematical derivation are correct.

However, there are many areas for improvement and improvement in the current work. First, the model's assumptions do not consider the cost of launching a BWH attack. Second, the modeling assumes that the two pools have the same computational power, which is not widely applicable. Therefore, we want to carry out the following in-depth research on this work in the future.

(1) We will consider the cost of launching the attack in the mining pool BWH attack modeling in the next step, which makes the game strategy perfect.

(2) We will study the mining decision-making strategy of double mining pools facing BWH attacks under different computational forces. Friedman's method [46,47] is utilized to find a stable solution by calculating the determinant of the Jacobian matrix for more than two mining pools. We intend to study this work in the following work further. At present, the basis of our work does not allow us to study this issue in depth, but we will conduct additional research in the subsequent work.

(3) In the next step, we plan to use PUF technology to build embedded clusters to solve the problem of optimal profit from BWH attacks on mining pools under the blockchain system.

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

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

Data Availability Statement: Not applicable

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

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

References

1. Bao, Q.; Li, B.; Hu, T.; Sun, X. A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work. *J. Syst. Softw.* **2023**, *196*, 111555–111580. [CrossRef]
2. Bendiab, G.; Hameurlaine, A.; Germanos, G.; Kolokotronis, N.; Shiaeles, S. Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. *IEEE Trans. Intell. Transp. Syst.* **2023**, *4*, 3614–3637. [CrossRef]
3. Xiao, P.; Salleh, M.I.; Zaidan, B.B.; Xuelan, Y. Research on risk assessment of Blockchain-driven Supply Chain finance: A systematic review. *Comput. Ind. Eng.* **2023**, *176*, 108990. [CrossRef]
4. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
5. Lee, T.F.; Lin, K.W.; Hsieh, Y.P.; Lee, K.C. Lightweight Cloud Computing-based RFID Authentication Protocols Using PUF for e-Healthcare Systems. *IEEE Sensors J.* **2023**, *6*, 6338–6349. [CrossRef]
6. binti Malik, M.; Zolkipli, M.F. Blockchain Threats: A Look into the Most Common Forms of Cryptocurrency Attacks. *Borneo Int. J.* **2023**, *1*, 20–32.
7. Nikhalat Jahromi, A.; Saghiri, A.M.; Meybodi, M.R. Nik Defense: An Artificial Intelligence Based Defense Mechanism against Selfish Mining in Bitcoin. *arXiv* **2023**, arXiv:2301.11463. [CrossRef]
8. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
9. Liu, F.; Li, Z.; Jia, K.; Xiang, P.; Zhou, A.; Qi, J.; Li, Z. Bitcoin Address Clustering Based on Change Address Improvement. *IEEE Trans. Comput. Soc. Syst.* **2023**, 1–12. [CrossRef]
10. Chen, Z.; Li, B.; Shan, X.; Sun, X.; Zhang, J. Discouraging pool block withholding attacks in Bitcoin. *J. Comb. Optim.* **2022**, *2*, 444–459. [CrossRef]
11. Zhang, Y.; Lv, X.; Chen, Y.; Ren, T.; Yang, C.; Han, M. FAWPA: A FAW Attack Protection Algorithm Based on the Behavior of Blockchain Miners. *Sensors* **2022**, *13*, 5032. [CrossRef]
12. Nikhalat-Jahromi, A.; Saghiri, A.M.; Meybodi, M.R. VDHLA: Variable Depth Hybrid Learning Automaton and Its Application to Defense against the Selfish Mining Attack in Bitcoin. *arXiv* **2023**, arXiv:2302.12096.
13. Singh, S.; Hosen, A.S.M.S.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
14. 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]
15. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confid. Comput.* **2022**, *2*, 1–20. [CrossRef]
16. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *2*, 100067. [CrossRef]
17. Monrat, A.A.; Schelen, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
18. Krichen, M.; Ammi, M.; Mihoub, A.; Almutiq, M. Blockchain for modern applications: A survey. *Sensors* **2022**, *14*, 5274. [CrossRef]
19. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Cao, Y. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
20. Xu, J.; Wang, C.; Jia, X. A Survey of Blockchain Consensus Protocols. *ACM Comput. Surv.* **2023**, *111*, 1–34. [CrossRef]
21. Zhang, B.; Kong, L.; Li, Q.; Min, X.; Liu, Y.; Che, Z. EB-BFT: An elastic batched BFT consensus protocol in blockchain. *Future Gener. Comput. Syst.* **2023**, *139*, 267–279. [CrossRef]
22. Wendl, M.; Doan, M.H.; Sassen, R. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *J. Environ. Manag.* **2023**, *326*, 116530. [CrossRef] [PubMed]
23. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *4*, 352–375. [CrossRef]
24. Moussa, M.; Beltrame, G. On the robustness of consensus-based behaviors for robot swarms. *Swarm Intell.* **2020**, *14*, 205–231. [CrossRef]
25. Bondugula, R.K.; Udgata, S.K.; Bommi, N.S. A Novel Weighted Consensus Machine Learning Model for COVID-19 Infection Classification Using CT Scan Images. *Arab J. Sci. Eng.* **2021**, *2021*, 1–12. [CrossRef]
26. Kenyeres, M.; Kenyeres, J. Distributed Mechanism for Detecting Average Consensus with Maximum-Degree Weights in Bipartite Regular Graphs. *Mathematics* **2021**, *9*, 3020. [CrossRef]
27. Meneghetti, A.; Sala, M.; Taufer, D. A survey on pow-based consensus. *Ann. Emerg. Technol. Comput. (AETiC)* **2020**, *1*, 8–18. [CrossRef]
28. Li, C.; Spychiger, F.; Tessone, C.J. The Miner's Dilemma with Migration: The Control Effect of Solo-Mining. *IEEE Trans. Netw. Serv. Manag.* **2022**. [CrossRef]
29. Praveen, G.; Singh, S.P.; Chamola, V.; Guizani, M. Novel Consensus Algorithm for Blockchain Using Proof-of-Majority (PoM). *IEEE Netw. Lett.* **2022**, *4*, 208–211. [CrossRef]
30. Ding, X.; Guo, J.; Li, D.; Wu, W. An incentive mechanism for building a secure blockchain-based internet of things. *IEEE Trans. Netw. Sci. Eng.* **2020**, *1*, 477–487. [CrossRef]

31. Sun, S.; Wang, W.; Xu, W.; Guo, J. Against Colluding Mining with Reward Sharing in MEC Empowered Mobile Blockchain System. In Proceedings of the 2022-IEEE International Conference on Communications (ICC), Seoul, Republic of Korea, 16–20 May 2022; pp. 4223–4228. [CrossRef]
32. Islam, M.D.; Shen, H.; Badsha, S. Integrating blockchain into supply chain safeguarded by PUF-enabled RFID. *Internet Things* **2022**, *18*, 100505. [CrossRef]
33. Huang, Z.; Wang, Q. A PUF-based unified identity verification framework for secure IoT hardware via device authentication. *World Wide Web* **2020**, *2*, 1057–1088. [CrossRef]
34. Lee, S.; Kim, S. Countering block withholding attack efficiently. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April 2019; pp. 330–335. [CrossRef]
35. Bag, S.; Ruj, S.; Sakurai, K. Bitcoin block withholding attack: Analysis and mitigation. *IEEE Trans. Inf. Forensics Secur.* **2016**, *8*, 1967–1978. [CrossRef]
36. Courtois, N.T.; Bahack, L. On subversive miner strategies and block withholding attack in bitcoin digital currency. *arXiv* **2014**, arXiv:1402.1718. [CrossRef]
37. Fujita, K.; Zhang, Y.; Sasabe, M.; Kasahara, S. Mining pool selection under block withholding attack. *Appl. Sci.* **2021**, *4*, 1617. [CrossRef]
38. Fujita, K.; Zhang, Y.; Sasabe, M.; Kasahara, S. Intelligent Mining Pool Selection in the Case of Unobservable Block Withholding Attack. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Virtual Conference, 3–6 May 2021; pp. 1–4. [CrossRef]
39. Chen, H.; Chen, Y.; Xiong, Z.; Han, M.; He, Z.; Liu, B.; Wang, Z.; Ma, Z. Prevention method of block withholding attack based on miners' mining behavior in blockchain. *Appl. Intell.* **2023**, *53*, 9878–9896. [CrossRef]
40. Kim, S.; Hahn, S.G. Mining pool manipulation in blockchain network over evolutionary block withholding attack. *IEEE Access* **2019**, *7*, 144230–144244. [CrossRef]
41. Can, B.; Hougaard, J.L.; Pourpouneh, M. On reward sharing in blockchain mining pools. *Games Econ. Behav.* **2022**, *136*, 274–298. [CrossRef]
42. Tuo, J.; Qin, G.; Shang, K.; Wang, Y. The Mining Selection in Multi-pools Under Block WithHolding Attack. In Proceedings of the 2022 41st Chinese Control Conference (CCC), Hefei, China, 25–27 July 2022; pp. 7454–7459. [CrossRef]
43. Wang, C.; Chu, X.; Qin, Y. Dissecting Mining Pools of Bitcoin Network: Measurement, Analysis and Modeling. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 398–412. [CrossRef]
44. Ren, M.; Guo, H.; Wang, Z. Mitigation of block withholding attack based on zero-determinant strategy. *PeerJ Comput. Sci.* **2022**, *8*, e997. [CrossRef]
45. Li, W.; Cao, M.; Wang, Y.; Tang, C.; Lin, F. Mining pool game model and nash equilibrium analysis for pow-based blockchain networks. *IEEE Access* **2020**, *8*, 101049–101060. [CrossRef]
46. Sigmund, K.; Nowak, M.A. Evolutionary game theory. *Curr. Biol.* **1999**, *9*, 503–505. [CrossRef] [PubMed]
47. Harper, M. Information Geometry and Evolutionary Game Theory. *arXiv* **2009**, arXiv:0911.1383. [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.