GenSelfHolding: Fusing Selfish Mining and Block Withholding Attacks on Bitcoin Revisited

Xuewen Dong[1], Sheng Gao[2]
[1]School of Computer Science & Technology, Xidian University, Xi'an 710071, China
[2]School of Information, Central University of Finance and Economics, Beijing 1008, China

Due to the monetary value of Bitcoin, the most influential digital cryptocurrency in the world, Bitcoin has naturally become a valuable target of attacks, resulting in the emergence of many attack strategies on it. Among those attack strategies, selfish mining and block withholding attacks are two typical ones and attackers can obtain higher revenues under certain conditions than with an honest mining strategy. However, the combination of them will be a new type and more serious attack, which has not been analyzed in depth. In this paper, we propose GenSelfHolding, a general combined attack model with one selfish mining pool and random multiple honest pools on Bitcoin. Based on Markov chain, a general state transition graph and a general state distribution probability are presented to describe the internal features of our model. A general principle is then provided to calculate the attacker's revenue. In addition, we give a detailed proof of the unique stable distribution of state transition probabilities. Such proof is an essential prerequisite for us to further present stable attacker revenue expressions under two specific scenarios, the GenSelfHolding model with two/three honest mining pools. Simulation results validate that the revenues of the attacker in these two specific models can reach up to 40% higher than those of classic selfish attackers in some cases.

Index Terms—**Bitcoin, Selfish mining attack, Block withholding attack, Combined attack, Markov chain.**

I. Introduction

Decentralized cryptocurrencies such as Bitcoin [1][2], Ethereum, Monero, and other altcoins have attracted the public's attention [3]. In April 2013, the Economist claimed that Bitcoin, regarded as "digital gold", has the potential to construct the future of payment and finance [4]. Based on cryptography and other secure techniques, Bitcoin has been the world's most popular electronic payment system due to its anonymity and decentralization [5] [6]. On Aug. 28, 2021, the value of one Bitcoin was $49,049.00

The underlying technology behind Bitcoin is blockchain, which is regarded as the trust machine by the Economist or in the industry [7]. It can build the peer-to-peer trust relationship among a set of nodes that distrust each other without the involvement of a trusted third party [8]. In the process of Bitcoin consensus namely Proof of Work (PoW), these network nodes are also termed as miners participant in the competition for the accounting right by solving a computational puzzle [9]. Any node that first gets the solution can package the transactions into a block and broadcast it to others. Once verified, it would be rewarded a certain amount of Bitcoin. This process for creating a new block is considered to be mining.

To implement a decentralized financial system, no centralized organization is allowed to exist in the Bitcoin protocol. However, Bitcoin is far from completely decentralized in practice [10]. Due to the limitation of a single mining node's computation power, the probability of successful mining is low, and the revenue is unstable. As a result, miners are inclined to unite into a mining pool for stable and higher revenues [11]. Thus, all miners in a pool will cooperate to mine and share revenue [12]. To a certain extent, this behavior violates the decentralization of Bitcoin and results in vulnerability [13] [14]. Besides undermining Bitcoin's principle of decentralization, mining pools has also been regarded as one of attack strategies' prerequisites.

Since cryptocurrencies such as Bitcoin are always accompanied by monetary value, they naturally become valuable attack targets. Among existing attack strategies [15] [16] against the Bitcoin protocol, selfish mining [17] [18] and block withholding [19] [20] are the two typical ones. Theoretically, an honest miner's revenue in the Bitcoin system is proportional to its computing power. However, contrast to an honest miner, higher revenues can be obtained by a dishonest miner with the selfish mining strategy. In a selfish mining attack, the fairness of the Bitcoin system will be attacked through a specific broadcasting block time strategy. After analyzing the characteristics of block generation, the authors in [17] utilize a state transition model to represent the selfish mining process of the Bitcoin network, deduce the probability of states, then derive the expected revenue of the attacker. Analysis results of the selfish mining strategy show that the computing power will gradually centralize, leading to selfish miners' domination of the entire Bitcoin network.

Another typical attack strategy in the Bitcoin protocol is the block withholding attack [21]. The attacking pool with a block withholding strategy takes out some computing power, whose action is somewhat similar to a "spy", in an honest pool. The spy-acting computing power will return its part of the revenue to the attacking pool. The authors of [22] model this attack strategy and give a detailed analysis of the attack revenue. As stated in [22], the total revenue of the pool will not be reduce by this strategy, whereas the honest pool will obtain a less revenue than deserved according to the proportion of computing power.

An attacker in the Bitcoin network may try any strategy to obtain more revenues. If a combined attack can return more

Manuscript received January 23, 2022; revised March 25, 2022. Corresponding author: Xuewen Dong (email: xwdong@xidian.edu.cn).

profits, the attacker tends to choose it. However, the combination of them is not sufficiently considered. Our previous work Ref. [23] have present a combined attack model "SelfHolding" by selfish mining and block withholding strategies. However, the random number of block withholding pools and thorough theoretical analysis of the attackers' revenue has not been considered. In this work, we rethink the combination of above two attack strategies in more depth and for a more general scenario, and propose a combined attack model, named GenSelfHolding, in which an attacking pool attacks multiple random honest pools. Theoretical analysis and experiments show that the attacker with our GenSelfHolding strategy can obtain up to 40% higher revenues than those with the general selfish mining strategy, within a certain range of computing power. The contribution of our work is as follows:

(1) We propose a general combined attack model, named GenSelfHolding with random multiple honest pools, on the original selfish mining attack and block withholding attack. Based on the architectural diagram of the general model, we provide the state transition diagram of the general model, and deduce the general state calculation expression and the general analysis principle of the attacker's revenue.

(2) To our knowledge, we are the first to give a detailed proof of the irreducibility, aperiodicity and state separability of the Markov chain in the state transition diagram. Based on those three properties, we can conclude that there is a unique stable distribution of state transition probabilities in that diagram, which is an essential prerequisite before deducing stable attacker revenue expressions.

*(3)*We present the attacker revenue expressions of our proposed model under two scenarios: two honest mining pools and three honest mining pools. Through the theoretical analysis and simulations, the attacker's practical revenues are in accordance with theoretical ones.

(4) We give detailed analyses of the influence of different factors, such as the attacker's entire computing power and the allocation proportion of computing power among attackers, on the attacker's revenues under different models. Moreover, revenue differences between the GenSelfHolding models under different scenarios are compared, with emphasis on changes in attackers' profitability.

This paper is organized as follows. In Section II, we briefly introduce the related works. In Section III, we propose our general combined attack model GenSelfHolding in detail. In Section IV and Section V, we verify our proposed model under two specific scenarios: the GenSelfHolding model with two honest mining pools and the GenSelfHolding model with three honest mining pools, and evaluate the factors affecting the attacker's revenue. Finally, we conclude this paper in Section VI.

II. Related Works

Cryptocurrencies, especially Bitcoin, have been a great success and attack strategies on Bitcoin have attracted researchers' interest [24]. We sketchily divide existing attack strategies into two categories, namely attacks from the Bitcoin backbone network [25] [26] and attacks on the Bitcoin protocol itself [27].

In attacks from the underlying network, DDoS attacks [28] and eclipse attacks [29] are the two most-typical attack strategies against the Bitcoin network. DDoS attacks are a common attack that exists in the Bitcoin and other networks [30]. The zombies, controlled by the attacker, send the victim a considerable volume of meaningless information, and halt the victim from carrying out normal network communication. The other classic attack strategy against the Bitcoin backbone network is the eclipse attack strategy, in which the attacker can control the communication channel between the victim and the Bitcoin nodes. As a result, the attacker's blockchain can easily become the longest chain and will be accepted by the victim, causing an increase in the profits of the attacker under certain conditions. EREBUS attack[31], an Eclipse-type attack, can partition and control the Bitcoin network through abundant network address resources between autonomous systems.

Besides, attacks are more threatening on the Bitcoin protocol itself than on the underlying network. Selfish mining attacks, block withholding attacks, FAW attacks and stubborn mining attacks are four classic attack strategies against the Bitcoin protocol. These four types of attack strategies are on the basis of the existence of mining pools. In the selfish mining attack, according to the difference between the public blockchain and his/her own private blockchain, the attacking pool or will not adopt different strategies to publish her newly discovered blocks. The stubborn mining, another typical Bitcoin mining attack, expands the strategic space of the selfish mining strategy. When the private chain of the stubborn mining attacker fails to lead in the race, that attacker will still mining on her private chain [32]. A stubborn mining pool at a disadvantage, under certain conditions, can turn into victory in the end. In a block withholding attack[22], the attacking pool takes out some computing power, which acts as a "spy", in an honest pool. The spy-acting computing power will return its part of the revenue to the attacking pool, leading to an increase in the attacker's revenue. Authors in [33] provide a detailed quantitative analysis of the monetary incentive that an attacker can earn by adopting a block withholding attack strategy, and they present a "sponsored block withholding attack" strategy that can effectively counter a block withholding attack in any mining pool. The FAW strategy [34] is a cooperative attacking approach. In the FAW strategy, some computing power is required to enter the victim mining pool and perform a block withholding attack. When the honest miner discovers a new block, attackers outside the victim mining pool will fork the blockchain. Through cooperation between the outside attackers and the inside "spy", the attacker can obtain higher revenues than by honest mining.

In one of our previous works Ref. [23], a combined attack model "SelfHolding" by selfish mining and block withholding strategies is proposed, in which we deduce and validate the revenue of the attacker under one selfish mining pool and limited honest pools with block withholding attackers. However, SelfHolding does not support random multiple pools with block withholding attackers. More over, theoretical analysis of the revenue calculation is missing, especially the proof that a stable distribution can be achieved by the Markov chain of the SelfHolding model with two honest mining pools, which is the foundation of revenue calculation.

In addition, in all the previously proposed models, only a small number of mining pools are considered. In this paper, we rethink the combination of above two attack strategies in more depth and for a more general scenario, and present a combined model GenSelfHolding under one selfish mining pool and random multiple honest mining pools with block withholding attackers. Moreover, we give a detail proof that the Markov chain of the SelfHolding model with two/three honest mining pools owns a stable distribution, and then validate the attacker revenues of our GenSelfHolding model under those two scenarios.

III. General Model Overview

In this section, we present the model of the GenSelfHolding attack strategy and provide the general state probability calculation formula and the principle of the attacker's revenue calculation. In this paper, we assume that authors have professional knowledge about Bitcoin mining process, and classic Bitcoin attack strategies, including the selfish mining attack strategy [17] and block withholding attack strategy [35].

A. Miners and Pools

Generally, the Bitcoin network contains a lot of miners with her own computing power, most of which are united into mining pools. In our GenSelfHolding attack model, there exists three kinds of miners, sketched as follows:

1) A selfish mining pool: The pool performs mining under the selfish mining strategy (i.e., lie in wait attack in [36]), which attackers maintain two blockchains: a public chain synchronizing with other Bitcoin users, and a private chain which contains new legal blocks are discovered and selectively published by the attacker for obtaining a higher revenue. Due to the private chain general leading the public chain, the selfish mining pool can increase her revenue with honest miners wasting their computing power. There is only one selfish mining pool in the GenSelfHolding attack model, with computing power $\alpha(0 < \alpha < 1)$.

2) Block withholding miners: In an honest pool, after miners discovering a new block and reporting to the pool manager, the pool manager will record the workload proof and share the revenues to all the miners. However, pretending to be an unlucky miner in a mining pool, the block witholding attacker in it just discards her new discovered blocks, which reduces the total revenue of the pool. It is noted that, in this paper, block withholding attack is same to the sabotage attack in [36].

In the GenSelfHolding attack model, the block withholding attackers' total computing power is denoted as $\tau(0 < \tau < 1)$.

3) Honest mining pools: In the GenSelfHolding model, without realizing the existence of attacking, honest mining pools are the victims of block withholding and selfish mining attacks. We use $\beta(0 < \beta < 1)$ to denote the sum of the honest mining pools' computing power in the GenSelfHolding model.

4) The relationship of miners: the sum of miners' computing powers is 1.

$$\alpha + \beta + \tau = 1. \tag{1}$$

The following relationship is satisfied by the above three characters, otherwise, the attacker can control the entire Bitcoin network, resulting in meaningless revenue analysis.

$$\alpha + \tau < \beta. \tag{2}$$

B. General Model

By exploiting the advantages of the selfish mining attack and block withholding attack, we propose a general combined attack model, GenSelfHolding, on one attacking pool and random multiple honest pools.

In Figure 1, as described earlier, the selfish mining pool's computing power is α. In addition, there are n honest mining pools, whose calculation power is expressed in terms of $\beta_k(1 \leq k \leq n)$. At the same time, there is one block withholding attacker in each honest mining pool. Each block withholding attacker attacks the honest mining pool where it locates. Reducing the revenue of honest miners, the block withholding attackers return the shared revenue to the selfish mining pool.

C. Representation of State

The general attack model can be abstracted as a Markov chain. Required by the Markov chain, we discuss the definition of state, state space, and transition probability.

- **State definition:** A state presents blockchains' length information and the blockchain fork information. Since there are several selfish mining pools besides of honest miners, a state is a tuple. Currently, there are two ways of expressing states: one regards the blockchain length difference information between the selfish attackers' private chains and the honest miners' public chain, and a superscript blockchain fork information as a state. The other way is to express the honest miner's public chain length, the attacker's private chain lengths, and a superscript blockchain fork information as a tuple [37]. In our combined attack model, the first method is used to describe the state. Since there exist multiple honest mining pools in our model, our state also appears as a tuple. For example, the state $(1, 1, ..., 1)$ indicates that the attackers' private chains overlength the honest miner's public chain by 1; the blockchain is not in a forked state at this time. The state $(0, 0, ..., 0)^{fork}$ represents that the attackers' private chains are consistent with the honest miner's public chain in length. However, the public chain and the private chain are in a forked state.
- **State transition probability:** While a new block is created/generated, the Markov chain will move from one state to another, which is an uncertain event for different start and end states. When establishing a Markov chain, it is necessary to give a transition probability between states. In our general model, the probability of transition between states is directly associated to the computing power of the attacker or of the honest mining pools.

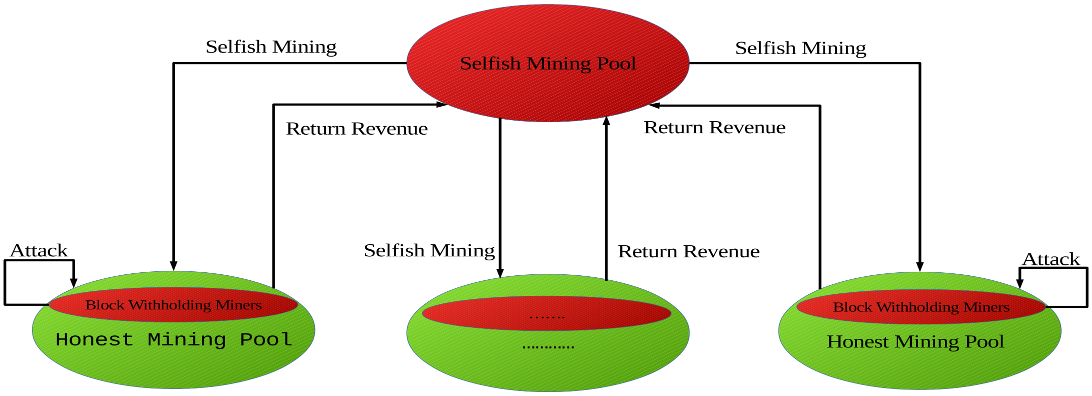

Fig. 1: GenSelfHolding model architecture diagram

D. General State Transition Diagram

We regard the general model as a Markov chain model and express the Markov chain as a state transition graph. Because the number of honest mining pools differs in different models, it cannot be represented by a single state; therefore we use a unified state $(0,0,...,0)^{fork}$ to represent the state of an attacker when the private chain of the attacker and the public chain of the honest mining pool are forked. The general state transition diagram is shown in Figure 2.

In Figure 2, the state transferring from state $(0,0,0..,0)$ to state $(1,1,1..,1)$ happens when the attacker finds a new block; thus the probability of this state transferring is α, the computing power of the attacker. The probability of state $(0,0,0..,0)^{fork}$ transferring to state $(0,0,0..,0)$ is denoted as p^{fork}. At this point, due to the emergence of new blocks, revenues of the attacking pool and honest mining pools appear, so the value of p^{fork} is critical to calculating the revenues of the attacker and honest pools under different specific scenarios.

Since self-loop states is allowed, our general state transition diagram of the GenSelfHolding model becomes a nonperiodic Markov chain. In the classic selfish mining strategy, the attacker's state transition diagram is a periodic Markov chain. In our GenSelfHolding model, the nonperiodic Markov chain is more likely to reach a stable state, which provides a certain extent of convenience when calculating state probabilities.

E. Calculation of State Probability

Because the revenue of the attacker and the honest mining pool is always generated when the state transitions, if you want to compute the attacker's expected revenue, you must first deduce the attacker's distribution probability. When the Markov chain model runs to a steady state, for each state, the probability of leaving that state is the same as the probability of entering it. Therefore, we can deduce the probability expression of each state. The specific expression is shown below.

$$\begin{cases} p^{fork}p((0,0,...,0)^{fork}) + (\sum_{i=1}^{n}\beta_i)p_{(k+1,k+1,...,k+1)} = \\ \alpha p(0,0,...,0) + (\sum_{i=1}^{n}\beta_i)p_{(k+1,k+1,...,k+1)} \\ \\ (\sum_{i=1}^{n}\beta_i + \tau_i)p_{(k+1,k+1,...,k+1)}p((0,0,0...,0)^{fork}) + \\ \alpha p((0,0,0...,0)^{fork}) = p^{fork}p((0,0,...,0)^{fork}) + \\ (\sum_{i=1}^{n}\beta_i + \tau_i) \\ \\ p_{(k+1,k+1,...,k+1)}p((0,0,0...,0)^{fork}) \\ \alpha p(0,0,...,0) + (\sum_{i=1}^{n}\beta_i)p(2,2,...,2) = \alpha p(1,1,...,1) \\ +(\sum_{i=1}^{n}\beta_i)p(1,1,...,1) \\ \\ \forall \text{k} \geq 2 : \alpha p_{(k,k,..k)} = (\sum_{i=1}^{n}\beta_i)p_{(k+1,k+1,...,k+1)} \end{cases} \tag{3}$$

In Equation (3), $p((0,0,...,0)^{fork})$ denotes the probability of the Markov chain being in state $(0,0,...,0)^{fork}$ after the Markov chain reaches a stable state, and p^{fork} represents the probability of transition from state $(0,0,...,0)^{fork}$ to state $(0,0,...,0)$. Other states can be deduced by analogy. The first formula in Equation (3) comes from the state flow balance of state $(0,0,0,...,0)^{fork}$. The second and third formulas imply the state flow balance of state $(1,1,1,...,1)$ and state $(0,0,0,...,0)$, respectively. The fourth formula expresses the state flow balance of state $(2,2,2,...,2)$ and the succeeding states.

The above formulas in Equation (3) can be simplified as follows:

$$\begin{cases} p^{fork}p((0,0,...,0)^{fork}) = \alpha p(0,0,...,0) \\ \\ (\sum_{i=1}^{n}\beta_i)p(1,1,...,1) = p^{fork}p((0,0,...,0)^{fork}) \\ \\ \alpha p(0,0,...,0) + (\sum_{i=1}^{n}\beta_i)p(2,2,...,2) = \alpha p(1,1,...,1) \\ +(\sum_{i=1}^{n}\beta_i)p(1,1,...,1) \\ \\ \forall \text{k} \geq 2 : \alpha p_{(k,k,..k)} = (\sum_{i=1}^{n}\beta_i)p_{(k+1,k+1,...,k+1)} \end{cases} \tag{4}$$

Since the sum of all states' probabilities is 1, the probability of each state can be calculated.

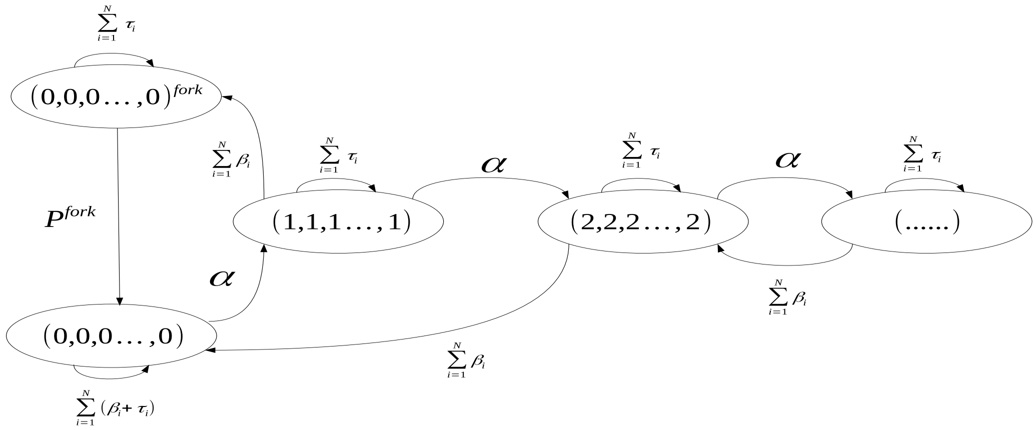

Fig. 2: General state transition diagram

F. Calculation Principle of Attacker's Revenue

Unlike the general state transition probability calculation, the calculation of the attacker's revenue cannot be expressed as a general formula, because the attacker's revenue is generated between specific state transitions with different transition probabilities, under GenSelfholiding models with different numbers of honest pools. Therefore, the analysis of the attacker's revenue must be specifically performed under each model. However, the calculation principle of the attacker's revenue can be given: when new blocks are generated, the number of new blocks belonging to the attack or the honest mining pools can be counted, and then the revenue of the attacker can be calculated.

IV. GENSELFHOLDING ATTACK MODEL WITH TWO HONEST POOLS

Considering that more than one mining pool may be attacked in reality, in this section, we present a specific attack model GenSelfHolding with two honest mining pools. We will verify the proposed GenSelfHolding attack model under this specific scenario and deduce the attacker's revenue.

It is noted that we have presented the revenue of the GenSelfHolding attack model with two honest pools in our previous work Ref. [23]. However, in Ref. [23], we do not provide the proof that the Markov chain of the SelfHolding model with two honest mining pools has a stable distribution, which is the foundation of revenue calculation. To guarantee the self-explanation property of this paper, we simply introduce the attack model and the revenue calculation of the attacker in this scenario, and then demonstrate revenue results with more details. Part of introduction sentences may be with high similarity to those in Ref. [23].

A. Attack Model

Figure 3 shows a specific GenSelfHolding model when the attacker attacks two honest mining pools. Pools A and B are two honest mining pools with computing power $\beta_1$and β_2, respectively. Pool C is a selfish mining pool with computing power α. D and E are two block withholding attackers with computing power τ_1 and τ_2, which respectively conduct block withholding attacks on A and B, and return the shared revenues to C. Meanwhile, C carries out selfish mining attacks on A and B, also resulting in the reduction of A's and B's revenues. In our GenSelfHolding attack model with two honest pools, $\gamma 1$ and γ_2 are used to denote the splitting coefficients of the two honest mining pools when the blockchain forks.

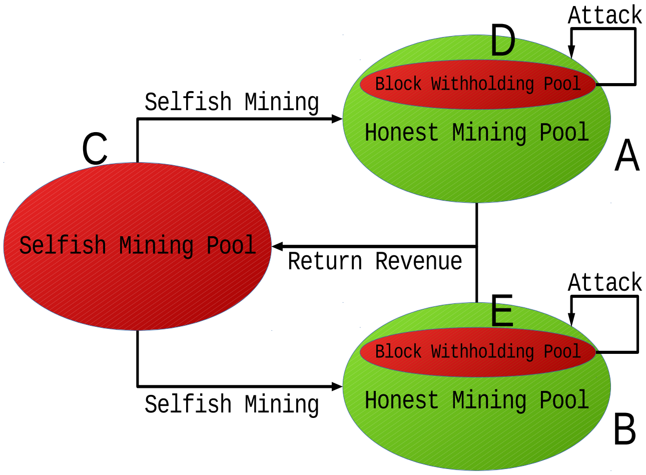

Fig. 3: Architecture of the GenSelfHolding model with two honest pools

Based on the classic selfish mining strategy, a selfish mining pool's actions are actually triggered by honest mining pools' actions. Since two honest pools are contained in this model, thus there exists two honest roles triggering selfish mining.

B. GenSelfHolding Attack Model with two honest pools

The GenSelfHolding attack model with two honest pools can be illustrated as a Markov chain model.

- **State space:** Due to the existence of two honest mining pools, a two-tuples and superscript are used to represent the state: $(L_a, L_b)^{fork}$. L_a, L_b respectively denote the length difference between the private chain of the attacker and the public chain of the first/second honest miner.

Based on the statement in Section III-C, $(0,0)^{''}$ implies that the second honest pool's public chain is forked by the private chain. While $(0,0)$ means that no fork exists at this time with the private chain consistent with the public chain.

- **State transition diagram:** The state transition diagram of the GenSelfHolding attack model with two honest pools is shown in Figure 4. The GenSelfHolding attack model takes two cases of blockchain forking into account, leading to the complexity of the state transition diagram.

$p_{(0,0)'}$ is used to denote the probability of the private blockchain detaching from the first honest pool. $p_{(1,1)}$ means the probability that the length difference between the private chain and the public chain is 1. As a result, the state probabilities satisfy the following equation.

$$\begin{cases} (\beta_1+\beta_2)p_{(1,1)} + \alpha p_{(1,1)} = \alpha p_{(0,0)} \\ (\beta_1+\beta_2)p_{(2,2)} = \alpha p_{(1,1)} \\ p_{(0,0)'} = \dfrac{\beta_1}{\alpha+\beta_1+\beta_2} p_{(1,1)} \\ p_{(0,0)''} = \dfrac{\beta_2}{\alpha+\beta_1+\beta_2} p_{(1,1)} \\ \forall \text{k} \geq 2 : \alpha p_{(k,k)} = (\beta_1+\beta_2)p_{(k+1,k+1)} \end{cases} \tag{5}$$

For Equation (5), the first formula implies the state flow balance of state $(1,1)$. The second, third and fourth formulas are derived from the flow balance of state $(2,2)$, state $(0,0)^{'}$ and state $(0,0)^{''}$, respectively. The last one indicates the flow balance of succeeding states.

Thus, we can obtain an expression for $p_{(1,1)}$.

$$p_{(1,1)} = \frac{\alpha(\beta_1+\beta_2-a)(\beta_1+\beta_2+a)}{2\alpha(\beta_1+\beta_2)^2 + (\beta_1+\beta_2-\alpha)(\beta_1+\beta_2+\alpha)^2}$$

Since other states' probabilities can be deduced from $p_{(1,1)}$. Thus, the probabilities of all states can be obtained.

C. Model Analysis

Based on the general state transition graph in Fig. 1, we can construct a state transition graph, as shown in Figure 4. Before we provide the revenues of attackers and honest pools, we need to prove that there is a stable distribution in the state transition graph. We will now prove some mathematical properties of the Markov chain in Figure 4.

Lemma 1. *The Markov chain of the GenSelfHolding model with two honest mining pools is an irreducible Markov chain.*

Proof. Using state (2, 2) as the cut point, Figure 4 is divided into two state sets. We use C_1 and C_2 to denote these two sets of states.

$$\begin{aligned} C_1 &= \{(0,0),(0,0)^{'},(0,0)^{''},(1,1)\} \\ C_2 &= \{(k,k)|k >= 3\} \end{aligned} \tag{6}$$

For state (2, 2), states to its left are a finite number of states and are ring-shaped, so the elements in set $C1$ and state (2,2) are all interlinked. According to the random process convention, we have

$$\exists n, p^{(n)}_{(i,i)(2,2)} > 0. \tag{7}$$

For the state to the right of the cut point, assuming that state (2, 2) continues to shift to the right, then,

$$\exists m, p^{(m)}_{(2,2)(j,j)} \geq \alpha^{(j-2)} > 0. \tag{8}$$

Similarly, it can be proved that the states on the right side of the cut point can reach state (2,2), so state (2,2) and the states on the right side are in an interworking relationship. From the above process, it can be directly proved that the states contained in the set C_1 and the set C_2 belong to the interworking relationship. For any two states $\{x, y : x \in C_1, y \in C_2\}$, the following expression can be obtained according to the C-K equation.

$$\exists(m,n), p[(x,x)(y,y)]^{m+n} = \sum_{k \in N^+} p[(x,x)(k,k)]p[(k,k)(y,y)]. \tag{9}$$

Substituting formula(7) and formula(8), we have the following expression.

$$\exists(m,n), p[(x,x)(y,y)]^{m+n} \geq p[(x,x)(2,2)]^m p[(2,2)(y,y)]^n. \tag{10}$$

This expression proves that set C_1 can be transferred to set C_2. Similarly, the reverse state transition is also provable. As a result, there is only one connected domain in the Markov chain abstracted by the simple GenSelfHolding model, and all states in this connected domain are bidirectionally interconnected. □

Lemma 2. *The Markov chain of the GenSelfHolding model with two honest mining pools is an aperiodic Markov chain.*

Proof. According to the definition of periodic Markov chain, it is necessary to prove that for any $i \in S$, there is a set of positive integers $\{n|n >= 1; p^{(n)}_{(i,i)(i,i)} > 0\}$ where the smallest n is the period of the Markov chain. For the Markov chain shown in Figure 4, for each state, there is the following state transition probability expression.

$$p^{(n)}_{(i,i)(i,i)} \geq \tau^n. \tag{11}$$

For any $i \in S$, there is a set of positive integers $\{n|n = 1; p^{(n)}_{(i,i)(i,i)} >= \tau > 0\}$. It can be proved that the Markov chain shown in Figure 4 is a Markov chain with a period of 1. According to the definition of nonperiodic Markov chain, the Markov chain abstracted by this GenSelfHolding model shown in Figure 4 is an aperiodic Markov chain. □

Lemma 3. *The Markov chain of the GenSelfHolding model with two honest mining pools is a Markov chain with state separability.*

Proof. Since the succeeding lemmas will split the state transition diagram of this GenSelfHolding model, divisibility of the state transition diagram needs to be proved. For state (2,2), we need to discuss the state split of its recurrence proof. We use $E_2(T)$ to denote the expected return time for state (2,2) and can deduce the following expression from the Markov property.

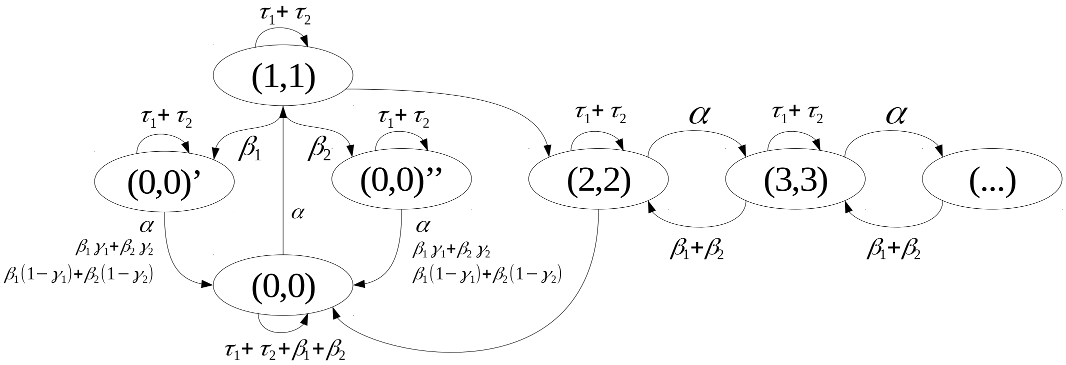

Fig. 4: State transition diagrams under the GenSelfHolding attack model with two honest pools

$$\begin{aligned}
&E_{(2,2)}(T) = E_{(2,2)}(T_{x_1=(2,2)}) + E_{(2,2)}(T_{x_1=(3,3)})\\
&+ E_{(2,2)}(T_{x_1=(0,0)})\\
&= p[(2,2)(2,2)] + p[(2,2)(3,3)]E_{(3,3)}(T)\\
&+ p[(2,2)(0,0)]E_{(0,0)}(T)\\
&= 1 + p[(2,2)(3,3)]E_{(3,3)}(T) + p[(2,2)(0,0)]E_{(0,0)}(T).
\end{aligned} \tag{12}$$

As seen from expression 12, the limited return time of state (2,2) depends on the limited return time of passing state (0,0) and passing state (3,3). Thus, for state (2,2), the limitation of its return time can be proved by splitting the state space. □

Lemma 4. *All states in the Markov chain of the GenSelfHolding model with two honest mining pools are normal reverse states.*

Proof. Since the divisibility of the state transition graph has been proved, the normal reversion of the transition graph can be investigated by means of the split of the transition graph. Examining the state transition of state (2,2), the chain can be divided into left and right parts. State (2,2) shifts to the left, and its shape is a finite state aperiodic Markov chain. According to the Markov chain finite normal return theorem [38], this chain must be a normal Markov chain; thus the time from state (2,2) to state (2,2) is a finite constant.

When state (2, 2) transitions to the left, it is a finite state and aperiodic Markov chain. To prove that the return time of state (2, 2) is limited, one only needs to prove that the return time of the transition to the right is limited. Hypothesis methods can be used to substitute verification. We use β instead of $\sum_{i=1}^{2}\beta_i$; we then have

$$v[(k,k)] = (1-\frac{\alpha}{\beta})(\frac{\alpha}{\beta})^{k-2}, \tag{13}$$

where $v(k)$ is based on the stochastic process convention and represents the stable distribution probability of the Markov chain in state k. The following uses the substitution method to verify the correctness of the conjecture. The correctness of formula 13 is verified below.

$$\sum_{k\in S} v[(k,k)]p[(k,k)(l,l)] = v[(j,j)]. \tag{14}$$

For $j = 2$

$$\begin{aligned}
&v[(2,2)]p[(2,2)(2,2)] + v[(3,3)]p[(3,3)(2,2)]\\
&= (1-\frac{\alpha}{\beta})(1-\alpha) + (1-\frac{\alpha}{\beta})(\frac{\alpha}{\beta})\beta\\
&= 1-\frac{\alpha}{\beta}.
\end{aligned} \tag{15}$$

For $j > 2$

$$\begin{aligned}
&v[(j-1),(j-1)]p[(j-1,j-1)(j,j)] + v[(j,j)]p[(j,j)(j,j)]\\
&+ v[(j+1,j+1)]p[(j+1,j+1)(j,j)]\\
&= (1-\frac{\alpha}{\beta})(\frac{\alpha}{\beta})^{k-2}.
\end{aligned} \tag{16}$$

The above shows that both Equation (15) and Equation (16) have stable distributions; therefore state (2,2) is the normal return state. According to the Markov chain connectivity theorem [38], all states in the Markov chain shown in figure 4 are normal return states. □

Theorem 1. *The Markov chain of the GenSelfHolding model with two honest mining pools has a stable distribution.*

Proof. Based on Markov's theorem [38] that a single connected domain, non-periodic, and normally return Markov chain must have a unique stable distribution, we can prove the theorem 1. □

D. Expected Revenues

After we prove that the Markov chain of the GenSelfHolding model with two honest mining pools has a stable distribution, then it is meaningful to calculate the expected revenues of the attackers and honest pools. According to the state transition diagram in Figure 4, the expression of each state can be deduced. Equation (17) is the expected revenue expression of the attackers and honest mining pools at this time. In Equation (17), $R_{honesttemp1}$ and $R_{honest1}$ means the temporary revenue and the final revenue of honest mining pool A, respectively. $R_{attacktemp}$ and $R_{attacker}$ are the temporary revenue and the final revenue of the attacker, respectively. We take the first formula $R_{honesttemp1}$ as an example to show the meaning of the revenue expression.

When the attacker's private chain forks with an honest mining pool's public chain and a new block is discovered in this honest mining pool, then this honest mining pool obtains the revenues of the two blocks. The first item $2p_{(0,0)'}\beta_1(1-\gamma_1)$ in the fist formula $R_{honesttemp1}$ reflects the obtained revenue in this situation.

When the attacker's private chain forks with an honest mining pool's public chain and another honest mining pool simultaneously discovers a new block, assuming that the new block is linked on the public chain, then the two honest mining pools obtain the revenues of a block. Conversely, if the new block link is on the private chain, then the attacker and the honest mining pool that discovered the new block each obtain a block of revenue. Items 2, 3, 4, and 5 of the first formula $R_{honesttemp1}$ reflect these situations.

When the public and private chains are not forked and a new block is discovered by an honest mining pool, the honest mining pool obtains the revenues of a new block. The last item in the first formula $R_{honesttemp1}$ corresponds to this situation.

$$\begin{cases} R_{honesttemp1} = 2p_{(0,0)'}\beta_1(1-\gamma_1) + p_{(0,0)'}\beta_2(1-\gamma_2) \\ +p_{(0,0)''}\beta_1(1-\gamma_1) + p_{(0,0)''}\beta_1\gamma_1 + p_{(0,0)'}\beta_1\gamma_1 + p_{(0,0)}\beta_1 \\ \\ R_{honesttemp2} = p_{(0,0)}\beta_2 + p_{(0,0)'}\beta_2\gamma_2 + p_{(0,0)'}\beta_2(1-\gamma_2) \\ +p_{(0,0)''}\beta_1(1-\gamma_1) + p_{(0,0)''}\beta_2\gamma_2 + 2p_{(0,0)''}\beta_2(1-\gamma_2) \\ \\ R_{attacktemp} = 2p_{(2,2)}(\beta_1+\beta_2) + p_{(i>2,i>2)}(\beta_1+\beta_2) \\ +2p_{(0,0)''}\alpha + 2p(0,0)'\alpha + p_{(0,0)''}\beta_2\gamma_2 + p_{(0,0)''}\beta_1\gamma_1 \\ +p_{(0,0)'}\beta_1\gamma_1 + p_{(0,0)'}\beta_2\gamma_2 \\ \\ R_{attacker} \\ = R_{attacktemp} + R_{honesttemp1}\dfrac{\tau_1}{\beta_1+\tau_1} + R_{honesttemp2}\dfrac{\tau_2}{\beta_2+\tau_2} \\ \\ R_{honest1} = R_{honesttemp1}\dfrac{\beta_1}{\beta_1+\tau_1} R_{honest2} = R_{honesttemp2}\dfrac{\beta_2}{\beta_2+\tau_2} \end{cases} \tag{17}$$

Here we dismiss the revenue result illustration of the attacker in this scenario, and readers can refer to Ref. [23] for a detailed revenue result illustration of the attacker. We also present some revenue results under this scenario comparing to the GenSelfHolding model with three honest pools in the next subsection.

E. Comparing with Classic Selfish Mining Model and Block Withholding Model

We try to determine the factors that influence the revenue of attackers under the GenSelfHolding attack model with two honest mining pools, the block withholding attack and the classic selfish mining. The default parameters are as follows: the splitting coefficients of honest miners are all set to 0.5, the total computing power of attackers is 0.2 and the computing power of selfish mining attacking is same to that of block withholding attacking, which means the computing power ratio between selfish mining and block withholding attacking is also 0.5.

Below, we compare the impact of the three models on the attacker's earnings on different aspects. In Figure 5 and the other evaluation figures, "sim" means the simulation results of revenue, and others represent the theoretical revenues. It is easy to find that the simulation revenues are nearly equal to the theoretical revenues, which verifies the correctness of the model analysis and revenue calculation.

- **Attacker's total power:** Firstly, we compare the revenues of attackers under three models on the attacker's total power.

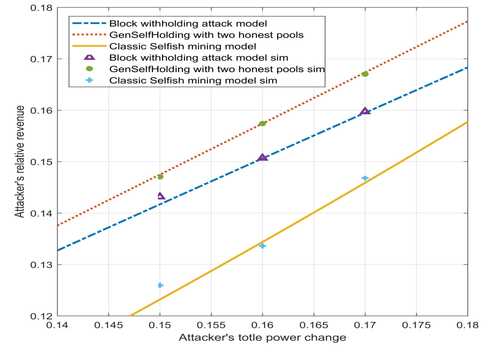

Fig. 5: The changes in the attacker's power under the GenSelfHolding attack model with two honest pools

In Figure 5, the GenSelfHolding model with two honest pools has higher revenues than the classic selfish mining model with small calculation power because at this time, the attacker's calculation power is too small to effectively perform selfish mining attacks. However, when the power of the attacker reaches a certain scale, the selfish mining attack will obtain higher revenues.

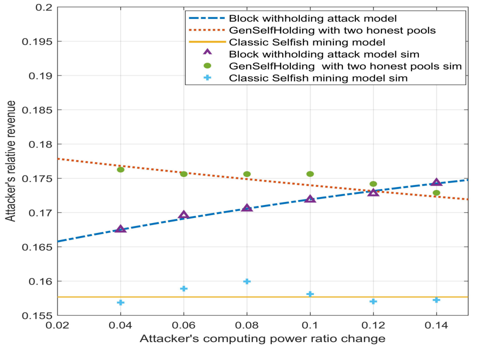

Fig. 6: The changes in attacker's power distribution under the GenSelfHolding attack model with two honest pools

- **Attacker's power distribution:** As depicted by Figure 6, when we fix the total power of the attacker and change the power ratio of the attacker's selfish mining and block withholding attacks, the attacker's revenue will also change significantly. In Figure 6, we fix the total power of the attacker to 0.1, and the GenSelfHolding attacker's revenue decreases as the attacker's power ratio increases. The classic selfish mining strategy does not include other attack strategies, so the attacker's revenues remain unchanged.
- **Splitting coefficient of honest mining pools:** As shown in Figure 7, when we fix other parameters and separately

change the splitting coefficient of the honest mining pools [39], the change in the attacker's revenue is also very different under the classic selfish mining model and the GenSelfHolding model with two honest mining pools. When the splitting coefficient of the honest mining pool becomes larger, the attacker's revenue will rise in either case, but when there are multiple honest mining pools, the attacker will have a greater probability of obtaining at least one block, leading to an increase in the revenue of the attacker.

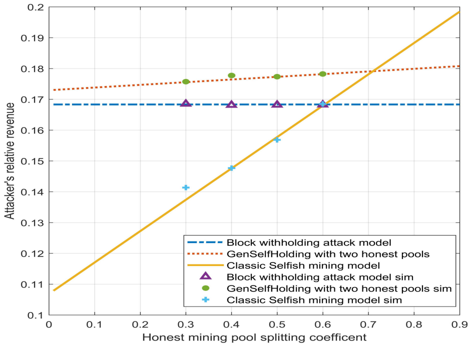

Fig. 7: The change in the Honest mining pool splitting coefficient under the GenSelfHolding model with two honest pools

V. GENSELFHOLDING ATTACK MODEL WITH THREE HONEST POOLS

In this section, we describe a specific GenSelfHolding attack scenario when a malicious mining pool attacks three honest mining pools.

A. Attack Model

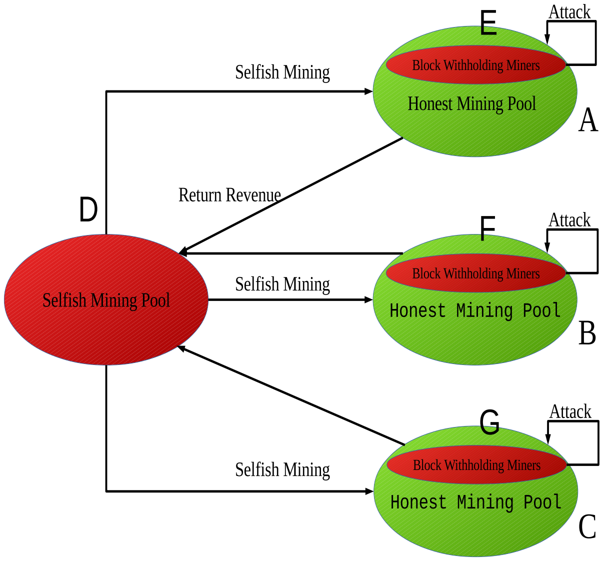

Fig. 8: Architecture of the GenSelfHolding attack model with three honest pools

Figure 8 shows the GenSelfHolding attack model with three honest mining pools. In this model, there exists a selfish mining pool denoted by D, and three honest mining pools marked A, B and C. There also are three block withholding attackers denoted E, F and G, which respectively conduct a block withholding attack on A, B and C, and return the shared revenues to D. Meanwhile, D carries out selfish mining attacks on A, B and C, which reduce the revenues of A, B and C, respectively.

B. State Space

Similar to the scenario in last section, the GenSelfHolding attack model with three honest pools can be expressed as a Markov chain model. We simply expand our state space because we have only one more honest mining pool compared to the GenSelfHolding model with two honest mining pools. In this situation, we use triples to represent the state. An additional fork state $(0,0,0)'''$ indicates the state of the third honest pool's public chain when it forks with the attacker's private chain.

C. State Transition Diagram

As shown in Figure 9, compared to the GenSelfHolding attack model in the last section, the GenSelfHolding model with three honest pools has only one more state $(0,0,0)'''$ to indicate that the public chain of the third honest mining pool has forked the attacker's private chain. There are two states $(0,0,0)$ in the state transition diagram, which makes our state transition diagram simpler. In fact, these two states are actually the same, when computing the probability of each state and deducing the attacker's revenue.

D. Revenue

In the GenSelfHolding model with three honest pools, the attacker's revenue expression is more complicated than that of the GenSelfHolding model with two honest pools. However, compared to the GenSelfHolding model with two honest pools, there is nearly no difference in how to calculate the attacker's revenue. From an intuitive point of view, because of more competition among honest mining pools, the profit of the attacker in this model is greater than in the GenSelfHolding model with two honest pools because when the public chain and the private chain are forked, the probability that the attacker can obtain at least one block becomes larger.

E. Model Analysis

For the GenSelfHolding model with three honest pools, the analysis is also carried out from two aspects: probability calculation and attacker revenue calculation. Before our analysis, we need to prove the stable distribution of the Markov chain of the GenSelfHolding model with three honest mining pools.

With a proof similar to Theorem 1, we have the following theorem:

Theorem 2. *The Markov chain of the GenSelfHolding model with three honest mining pools has a stable distribution.*

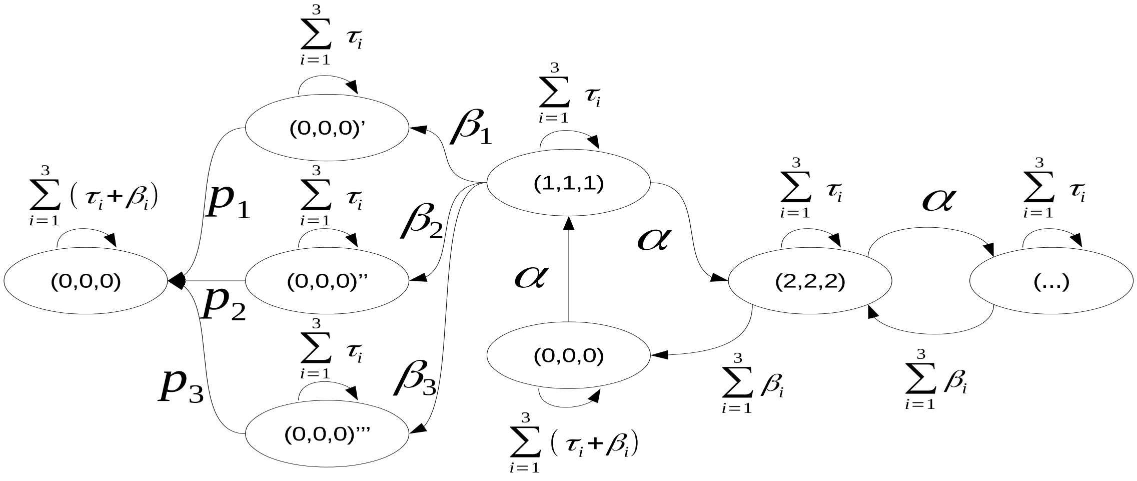

Fig. 9: State transition diagram under the GenSelfHolding attack model with three honest pools

F. Probability Calculation

Under the GenSelfHolding model with three honest pools, the method of calculating each state in the state transition diagram is similar to that of the GenSelfHolding model with two honest pools. When we set some variables in the expression to 0, the calculation expression of each state will be the same as that of the GenSelfHolding model with two honest pools. For the sake of brevity, we use p_1, p_2 and p_3 to indicate the corresponding state transition probabilities in Figure 9. We then have

$$\begin{cases} (\alpha+\beta_1+\beta_2+\beta_3)p_{(0,0,0)'}=\beta_1 p_{(1,1,1)} \\ (\alpha+\beta_1+\beta_2+\beta_3)p_{(0,0,0)''}=\beta_2 p_{(1,1,1)} \\ (\alpha+\beta_1+\beta_2+\beta_3)p_{(0,0,0)'''}=\beta_3 p_{(1,1,1)} \\ (\beta_1+\beta_2+\beta_3)p_{(1,1,1)}+\alpha p_{(1,1,1)}=\alpha p_{(0,0,0)} \\ \alpha p_{(1,1,1)}=(\beta_1+\beta_2+\beta_3)p_{(2,2,2)} \\ (\alpha+\beta_1+\beta_2+\beta_3)(p_{(0,0,0)'}+p_{(0,0,0)''}+p_{(0,0,0)'''})+ \\ (\beta_1+\beta_2+\beta_3)p_{(2,2,2)}=\alpha p_{(0,0,0)} \\ \forall \text{k}\geq 2:\alpha p_{(k,k,k)}=(\beta_1+\beta_2+\beta_3)p_{(k+1,k+1,k+1)}. \end{cases} \tag{18}$$

In Equation (18), the first, second, and third formulas are derived from the state flow balance of state $(0,0,0)^{'}$, state $(0,0,0)^{''}$ and state $(0,0,0)^{'''}$, respectively. The fourth and fifth formulas imply the state flow balance of state $(1,1,1)$ and state $(2,2,2)$, respectively. The sixth represents the flow balance of state $(0,0,0)$. The seven formulas are derived from the state flow balance of state $k(k\geq 2)$. We can deduce the distribution probability $p_{(1,1,1)}$, which is the probability of state $(1,1,1)$ in Figure 9.

$$\begin{cases} \dfrac{1}{p_{(1,1,1)}}=\dfrac{\beta_1+\beta_2+\beta_3}{\alpha+\beta_1+\beta_2+\beta_3}+\dfrac{\alpha+\beta_1+\beta_2+\beta_3}{\alpha} \\ +\dfrac{\beta_1+\beta_2+\beta_3}{\beta_1+\beta_2+\beta_3-\alpha}. \end{cases} \tag{19}$$

Concerning the probability distribution of other states, we use the state $p_{(1,1,1)}$ to calculate. Thereafter, we can compute the probability expressions of p_1, p_2 and p_3.

$$\begin{cases} p_1=p_{(0,0,0)'}\alpha+p_{(0,0,0)'}\beta_1\gamma_1+p_{(0,0,0)'}\beta_1(1-\gamma_1) \\ +p_{(0,0,0)'}\beta_2\gamma_2+p_{(0,0,0)'}\beta_2(1-\beta_2)+p_{(0,0,0)'}\beta_3\gamma_3 \\ +p_{(0,0,0)'}\beta_3(1-\gamma_3) \\ p_2=p_{(0,0,0)'}\alpha+p_{(0,0,0)''}\beta_1\gamma_1+p_{(0,0,0)''}\beta_1(1-\gamma_1) \\ +p_{(0,0,0)''}\beta_2\gamma_2+p_{(0,0,0)''}\beta_2(1-\beta_2)+p_{(0,0,0)''}\beta_3\gamma_3 \\ +p_{(0,0,0)''}\beta_3(1-\gamma_3) \\ p_3=p_{(0,0,0)'''}\alpha+p_{(0,0,0)'''}\beta_1\gamma_1+p_{(0,0,0)'''}\beta_1(1-\gamma_1) \\ +p_{(0,0,0)'''}\beta_2\gamma_2+p_{(0,0,0)'''}\beta_2(1-\beta_2)+p_{(0,0,0)'''}\beta_3\gamma_3 \\ +p_{(0,0,0)'''}\beta_3(1-\gamma_3). \end{cases} \tag{20}$$

In Equation (20), the first formula is to compute the transition probability of state $(0,0,0)^{'}$ to state $(0,0,0)$. The next two formulas are the transition probabilities of state $(0,0,0)^{'}$ to state $(0,0,0)$ and of state $(0,0,0)^{'''}$ to state $(0,0,0)$.

G. Attacker's Revenue Calculation

Under this model, the attacker's revenue calculation is more complicated than that of the GenSelfHolding model with two honest pools. With the addition of an honest mining pool, when the blockchain is forked, the attacker's revenue calculation needs to be careful to distinguish between different situations. The attacker's specific revenue can be deduced as Equation 21.

$$
\left\{
\begin{aligned}
&R_{honesttemp1} = p_{(0,0,0)}\beta_1 + 2p_{(0,0,0)'}\beta_1(1-\gamma_1)\\
&+p_{(0,0,0)'}\beta_1\gamma_1 + p_{(0,0,0)'}\beta_2(1-\gamma_2) + p_{(0,0,0)'}(1-\gamma_3)\\
&+p_{(0,0,0)''}\beta_1\gamma_1 + p_{(0,0,0)''}\beta_1(1-\gamma_1) + p_{(0,0,0)'''}\beta_1\gamma_1\\
&+p_{(0,0,0)'''}\beta_1(1-\gamma_1)\\
&\\
&R_{honesttemp2} = p_{(0,0,0)}\beta_2 + 2p_{(0,0,0)''}\beta_2(1-\gamma_2)\\
&+p_{(0,0,0)''}\beta_2\gamma_2 + p_{(0,0,0)''}\beta_1(1-\gamma_1) + p_{(0,0,0)''}\beta_3(1-\gamma_3)\\
&+p_{(0,0,0)'}\beta_2\gamma_2 + p_{(0,0,0)'}\beta_2(1-\gamma_2) + p_{(0,0,0)'''}\beta_2\gamma_2\\
&+p_{(0,0,0)''}\beta_2(1-\gamma 2)\\
&\\
&R_{honesttemp3} = p_{(0,0,0)}\beta_3 + 2p_{(0,0,0)'''}\beta_3(1-\gamma_3)\\
&+p_{(0,0,0)'''}\beta_3\gamma_3 + p_{(0,0,0)'''}\beta_1(1-\gamma_1)\\
&+p_{(0,0,0)'''}\beta_2(1-\gamma_2) + p_{(0,0,0)'}\beta_3(1-\gamma_3)\\
&+p_{(0,0,0)'}\beta_3\gamma_3 + p_{(0,0,0)''}\beta_3(1-\gamma_3) + p_{(0,0,0)''}\beta_3\gamma_3\\
&\\
&R_{tmpa} = 2p_{(2,2,2)}(\beta_1+\beta_2+\beta_3) + p_{(k,k,k)}(\beta_1+\beta_2+\beta_3)\\
&+2\alpha p_{(0,0,0)'} + p_{(0,0,0)'}\beta_1\gamma_1 + p_{(0,0,0)'}\beta_2\gamma_2\\
&+p_{(0,0,0)'}\beta_3\gamma_3 + 2\alpha p_{(0,0,0)''} + p_{(0,0,0)''}\beta_2\gamma_2\\
&+p_{(0,0,0)''}\beta_3\gamma_3 + p_{(0,0,0)''}\beta_1\gamma_1 + 2\alpha p_{(0,0,0)'''}\\
&+p_{(0,0,0)'''}\beta_3\gamma_3 + p_{(0,0,0)'''}\beta_1\gamma_1 + p_{(0,0,0)'''}\beta_2\gamma_2\\
&R_{honest1} = R_{honesttemp1}(\frac{\beta_1}{\tau_1+\beta_1})\\
&R_{honest2} = R_{honesttemp2}(\frac{\beta_2}{\tau_2+\beta_2})\\
&R_{honest3} = R_{honesttemp3}(\frac{\beta_3}{\tau_3+\beta_3})\\
&R_{attacker} = R_{tmpa} + R_{honesttemp1}(\frac{\beta_1}{\beta_1+\tau_1})\\
&+R_{honesttemp2}(\frac{\beta_2}{\beta_2+\tau_2}) + R_{honesttemp3}(\frac{\beta_3}{\beta_3+\tau_3}).
\end{aligned}
\right.
\tag{21}
$$

Equation (21) is really hard to understand, but the principles of its calculation are not difficult. We next take $R_{honesttemp1}$ as an example to explain, and other expressions can be understood in a similar way.

When the attacker's private chain does not fork with the honest miner's public chain, and an honest miner discovers a new block, then the honest mining pool can obtain a revenue of the new block. The first item $p_{(0,0,0)}\beta_1$ of $R_{honesttemp1}$ in Equation (21) reflects this scenario.

When the private chain of the attacker forks with the public chain of an honest mining pool, and the honest miner, who accepts the public chain as a legal blockchain, discovers a new block, then the honest mining pool obtains the revenue of the two blocks. On the other hand, if an honest mining pool accepting the private chain as the legal blockchain discover new blocks, then both the attacker and the honest mining pool obtains the revenue of one block. Items 2, 3, 4, and 5 of $R_{honesttemp1}$ reflect these possibilities.

When the public chain of other honest mining pools and the private chain of the attacker are forked, other mining pools may choose to accept the honest mining pool's public chain as a legal blockchain. At this time, each of the two honest mining pools obtains one block. However, if the other honest mining pools believe that the attacker's private chain is a legal blockchain, then both the attacker and other honest mining pools obtain the revenue of one block. The remaining items of $R_{honesttemp1}$ reflect these possibilities.

It can be found from the attacker's revenue expression that the attacker's revenue is affected by more factors than that of the GenSelfHolding model with two honest mining pools.

H. Comparing with the GenSelfHolding model with Two Honest Mining Pools

From an intuitive point of view, when the number of honest mining pools increases, the chances of an attacker gaining at least one block will also increase. However, contrary to intuition, in many cases, as the number of honest mining pools increases, the revenue of the attacker will decline. The default parameter setting is same to that in Section IV-E.

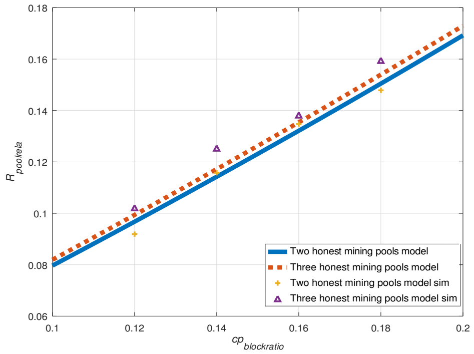

Fig. 10: The changes in the attacker's power under the GenSelfHolding attack model with three honest pools

- **Attacker's total power change:** From the given attacker's revenue expression, we can predict that when the attacker's total calculation power changes, whether it is the GenSelfHolding model with two honest pools or the GenSelfHolding model with three honest pools, the attacker's revenue is the same. We verified this idea through experiments, and the experimental results are shown in Figure 10.
  In Figure 10, since the revenue of the attacker under the GenSelfHolding model with two honest pools is exactly the same as that of the attackers under the GenSelfHolding model with three honest pools, two different types of lines are used to represent the revenue of the attackers under the two models.
- **Honest mining pool calculation power distribution:** When the calculation power distribution among honest mining pools changes, the attacker's revenue will also fluctuate greatly.
  As shown in Figure 11, when the computation power distribution between honest mining pools changes, the attacker's revenue changes under the two models are similar. However, no matter how similar the changes are, the attacker's benefit under the GenSelfHolding model with two honest pools is greater than that under the GenSelfHolding model with three honest pools.
- **Attacker power distribution ratio change:**
  Figure 12 shows that when we fix the attacker's total power to 0.3 and other parameters are unchanged, the

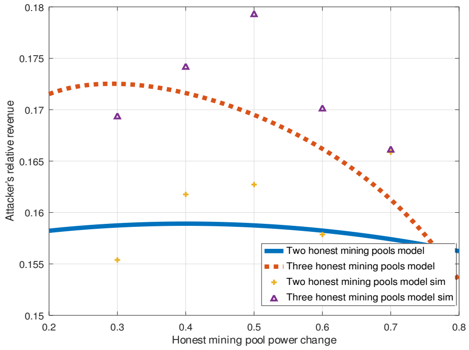

Fig. 11: The change in honest mining pool calculation power distribution under the GenSelfHolding model with three honest pools

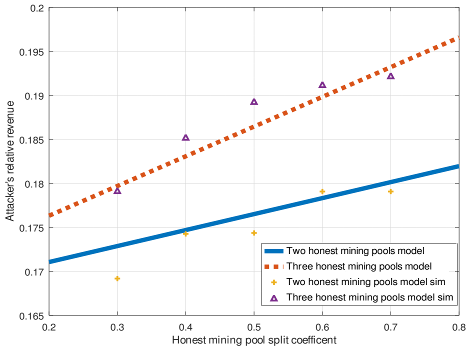

Fig. 12: The change in attacker power distribution ratio under the GenSelfHolding model with three honest pools

revenue of the attacker under the GenSelfHolding model with two honest pools is greater than that under the GenSelfHolding model with three honest pools.

VI. Conclusion

Serious security problems exist in the Bitcoin system; selfish mining and block withholding attacks are two of the most classic attack in this field. In this paper, we present a general model, GenSelfHolding, with a combined attack strategy on these two attack strategies. We investigate the stable distribution property, consisting of the irreducibility, aperiodicity and state separability of state transition probabilities in this general model. In addition, we verify our model under two specific scenarios and find that within a certain range of computing power, the attackers' revenue show different changes and that more revenues can be obtained by the attacker under this GenSelfHolding attack strategy in some cases.

VII. Acknowledgment

This work is supported in part by National key R&D Program of China(No. 2020YFB1005500), in part by National Natural Science Foundation of China (No. 61972310, 61972017, 62072487), in part by Populus Euphratica Found (No.CCF-HuaweiBC2021008).

References

[1] Reuben Grinberg. Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, 4:159, 2012.

[2] Lam Pak Nian and David LEE Kuo Chuen. Introduction to bitcoin. In *Handbook of Digital Currency*, pages 5–30. Elsevier, 2015.

[3] Jun Zou, Bin Ye, Lie Qu, Wang Yan, Mehmet A. Orgun, and Li Lei. A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. *IEEE Transactions on Services Computing*, PP(99):1–1, 1939.

[4] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[5] Yinghui Zhang, Robert Deng, Ximeng Liu, and Zheng Dong. Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Transactions on Services Computing*, PP(99):1–1, 1939.

[6] Ruinian Li, Tianyi Song, Mei Bo, Li Hong, Xiuzhen Cheng, and Limin Sun. Blockchain for large-scale internet of things data storage and protection. *IEEE Transactions on Services Computing*, PP(99):1–1, 1939.

[7] Zhu Xinghui, Zheng Jiawei, Ren Baoquan, Dong Xuewen, and Yulong Shen. Microthingschain: Blockchain-based controlled data sharing platform in multi-domain iot. *Journal of Networking and Network Applicationst*, 1(1):19–27, 2021.

[8] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on*, pages 557–564. IEEE, 2017.

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. whitepaper, 2009, 2009.

[10] Alireza Beikverdi and JooSeok Song. Trend of centralization in bitcoin's distributed network. In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on*, pages 1–6. IEEE, 2015.

[11] Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pages 919–927. International Foundation for Autonomous Agents and Multiagent Systems, 2015.

[12] Meni Rosenfeld. Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*, 2011.

[13] Chinmay A Vyas and Munindra Lunagaria. Security concerns and issues for bitcoin. In *the proceedings of National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB-2014*, 2014.

[14] Yujuan Wen, Fengyuan Lu, Yufei Liu, and Xinli Huang. Attacks and countermeasures on blockchains: A survey from layering perspective. *Computer Networks*, 191:107978, 2021.

[15] Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, and Min Suk Kang. A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network. In *Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P)*, 2020.

[16] S. Zhang and J. Lee. Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*, 15(10):5715–5722, 2019.

[17] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102, 2018.

[18] Hongyue Kang, Xiaolin Chang, Runkai Yang, Jelena Mišić, and Vojislav B. Mišić. Understanding selfish mining in imperfect bitcoin and ethereum networks with extended forks. *IEEE Transactions on Network and Service Management*, pages 1–1, 2021.

[19] Alireza Toroghi Haghighat and Mehdi Shajari. Block withholding game among bitcoin mining pools. *Future Generation Computer Systems*, 97:482–491, 2019.

[20] Shuya Feng, Jia He, and Maggie X. Cheng. Security analysis of block withholding attacks in blockchain. In *ICC 2021 - IEEE International Conference on Communications*, pages 1–6, 2021.

[21] Deepak K. Tosh, Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, and Laurent Njilla. Security implications of blockchain cloud with analysis of block withholding attack. In *IEEE/ACM International Symposium on Cluster*, 2017.

[22] Ittay Eyal. The miner's dilemma. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 89–103. IEEE, 2015.

[23] Xuewen Dong, Feng Wu, Anter Faree, Deke Guo, Yulong Shen, and Jianfeng Ma. Selfholding: A combined attack model using selfish mining with block withholding attack. *Computers&Security*, 87:101584, 2019.

[24] Jennifer J. Xu. Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):25, 2016.

[25] Danny Bradbury. The problem with bitcoin. *Computer Fraud & Security*, 2013(11):5–8, 2013.

[26] Joan Antoni Donet Donet, Cristina Pérez-Sola, and Jordi Herrera-Joancomartí. The bitcoin p2p network. In *International Conference on Financial Cryptography and Data Security*, pages 87–102. Springer, 2014.

[27] Ghassan Karame. On the security and scalability of bitcoin's blockchain. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1861–1862. ACM, 2016.

[28] Amir Feder, Neil Gandal, JT Hamrick, and Tyler Moore. The impact of ddos and other security shocks on bitcoin currency exchanges: Evidence from mt. gox. *Journal of Cybersecurity*, 3(2):137–144, 2018.

[29] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. In *USENIX Security Symposium*, pages 129–144, 2015.

[30] Shaohan Feng, Wenbo Wang, Zehui Xiong, Dusit Niyato, Wang Ping, and Shaun Shuxun Wang. On cyber risk management of blockchain networks: A game theoretic approach. *IEEE Transactions on Services Computing*, PP(99):1–1, 2018.

[31] Muoi Tran, In Sang Choi, Gi Jun Moon, Anh V. Vu, and Min Suk Kang. A stealthier partitioning attack against bitcoin peer-to-peer network. pages 894–909, 2020.

[32] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, pages 305–320. IEEE, 2016.

[33] S. Bag, S. Ruj, and K. Sakurai. Bitcoin block withholding attack: Analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, 12(8):1967–1978, Aug 2017.

[34] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 195–209. ACM, 2017.

[35] Nicolas T Courtois and Lear Bahack. On subversive miner strategies and block withholding attack in bitcoin digital currency. *arXiv preprint arXiv:1402.1718*, 2014.

[36] Meni Rosenfeld. Analysis of bitcoin pooled mining reward systems. *CoRR*, abs/1112.4980, 2011.

[37] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.

[38] Rick Durrett. Probability: Theory and examples. *Cambridge U Press*, 39(5):320–353, 2005.

[39] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pages 1–10. IEEE, 2013.