BM-PAW: A Profitable Mining Attack in the PoW-based Blockchain System

Junjie Hu and Na Ruan [✉]

Department of Computer Science and Engineering, Shanghai Jiao Tong University,
Shanghai 200240, China
{nakamoto, naruan}@sjtu.edu.cn

Abstract. Mining attacks enable an adversary to procure a disproportionately large portion of mining rewards by deviating from honest mining practices within the PoW-based blockchain system. In this paper, we demonstrate that the security vulnerabilities of PoW-based blockchain extend beyond what these mining attacks initially reveal. We introduce a novel mining strategy, named BM-PAW, which yields superior rewards for both the attacker and the targeted pool compared to the state-of-the-art mining attack, PAW. BM-PAW attackers are incentivized to offer appropriate bribe money to other targets, as they comply with the attacker's directives upon receiving payment. We further find the BM-PAW attacker can circumvent the "miner's dilemma" through equilibrium analysis in a two-pool BM-PAW game scenario, wherein the outcome is determined by the attacker's mining power. We finally propose practical countermeasures to mitigate these novel pool attacks.

Keywords: Proof of Work; Blockchain; Mining Attack; Selfish Mining; Power Adjusting Withholding; Mining Game

1 Introduction

Bitcoin [1], a decentralized cryptocurrency grounded in blockchain technology, was introduced by Satoshi Nakamoto in November 2008. Distinct from conventional currencies, Bitcoin does not depend on designated currency institutions for issuance. Instead, it is produced through extensive computations in accordance with predefined algorithms. The PoW-based blockchain system employs a distributed database encompassing numerous nodes across the entire peer-to-peer network to verify and record all transactions. It also adopts cryptographic designs to safeguard the security of the entire currency circulation process. The decentralization of the peer-to-peer network and consensus algorithms ensures that the currency value cannot be artificially manipulated through the mass creation of PoW-based blockchain. The cryptographic-based designs allow PoW-based tokens to be transferred or paid for solely by its rightful owners.

In the PoW-based blockchain system, participants known as miners can obtain rewards by appending transaction records to the ledger, referred to as the blockchain. This process necessitates miners solving cryptographic puzzles, serving as a proof of work [2]. The miner who first solves the puzzle and generates a

valid block is eligible to receive block rewards, which amounted to 3.125 Bitcoins in November 2024. This activity of solving cryptographic puzzles and generating blocks is termed the "mining process". Occasionally, due to network communication delays, two or more blocks may be generated and published simultaneously, leading to a fork in the blockchain. To ensure consistency, the system selects one of these branches to ultimately become the main chain. Upon recognizing the longest chain, miners on other branches redirect their attention and mining power to the main chain. In the Bitcoin system, the difficulty of solving cryptographic puzzles is adjusted every two weeks to maintain a constant average block generation time of approximately 10 minutes. However, given the current mining power's hash rate exceeding 3.3×10^{20} Hash/s [3], it may take an individual miner several months or even years to solve a mining puzzle [4]. Consequently, to achieve stable income, miners tend to unite and form mining pools. Most mining pools have a designated pool manager who is responsible for allocating tasks and distributing rewards. When a mining pool discovers a block, the reward is shared among the pool's miners based on their contributions, specifically the number of shares they have submitted.

Cryptocurrencies, possessing intrinsic monetary value, inherently become a lucrative target for cyberattacks. Despite the robust security design of PoW-based blockchain, prior research has demonstrated that it may be more financially beneficial for an attacker to deviate from honest mining strategies. Such deviations include adopting higher-level mining tactics associated with selfish mining [5,6,7,8], engaging in block withholding (BWH) [9], executing fork after withholding (FAW) [10], and employing power adjusting withholding (PAW) [11].

In this paper, we introduce a novel mining attack targeting pool mining, called Power Adjusting Withholding Attack with Bribe Money (BM-PAW), which promises the attacker greater profits than those attainable through PAW attack. Our underlying insight is that it is beneficial for the attacker to offer an appropriate bribe to other miners, as these miners may comply with the attacker's directives if they accept the payment. We term such payment "bribe money" (BM) and refer to the induced miners as the "target pool". It is important to note that BM differs from bribery in the context of bribery selfish mining (BSM). For example, the attacker in our scenario has the authority to instruct the target pool to discard the Full Proof of Work (FPoW) or mine on the attacker's branch. BM-PAW extends the traditional PAW attack by incorporating a unique mining strategy centered on BM. The rationale behind BM-PAW is that the attacker consistently achieves additional profits when they possess greater mining power or their competitor has lesser mining power. In BM-PAW, the attacker initially infiltrates the target pool to persuade it to accept the bribe and participate in the BM-PAW attack. During this phase, the attacker negotiates with the target pool to determine the proportion of the reward that will be offered as BM per block. Once the target accepts the bribe, it must adhere to the attacker's instructions, either mining on the attacker's FPoW or discarding blocks in different forking competitions. We demonstrate that with the appropriate selection of BM, it is feasible to achieve incentive compatibility between

the attacker and the target pool. Specifically, both the target and the attacker can obtain higher rewards than those attainable through PAW.

In this paper, we propose and discuss the following vital questions:

- *First, how to adjust the attacker's infiltration mining power to maximize his rewards?*
- *Moreover, how to choose the proper bribe money to achieve incentive compatibility between the attacker and the target pool?*
- *Finally, what equilibrium will the BM-PAW game of different types of participants eventually reach?*

1.1   Our Contributions

In our research, we introduce a novel mining attack denominated as BM-PAW. In this attack scenario, the attacker is incentivized to offer an appropriate amount of bribe money to a target pool, which in turn discards forks or mines on the attacker's FPoW. To address the initial inquiry, we derive the expected reward for the attacker and formulate the optimal infiltration mining power adjustment by solving the corresponding optimization equation. Our quantitative analysis and simulations reveal that both the attacker and the target pool can achieve higher rewards compared to the advanced and profitable mining attack known as PAW. This finding underscores the vulnerability of pooled mining in the PoW-based blockchain network.

Subsequently, we undertake a formal analysis of the BM-PAW attack across various scenarios. Our analysis specifically focuses on both a singular victim pool and a game involving multiple BM-PAW attackers. To address the second question, we individually scrutinize the rewards accrued by both the attacker and the target pool. We incorporate the constraints that the minimum bribe amount must suffice to ensure the target pool's reward in BM-PAW exceeds that in PAW, while the maximum bribe amount must guarantee that the attacker's reward in BM-PAW is greater than in PAW. Furthermore, we demonstrate that with an apt selection of bribe money, it is feasible to attain incentive compatibility between the attacker and the target pool, fostering a mutually beneficial outcome. Concurrently, simulations corroborate that with an appropriate bribe amount, both the BM-PAW attacker and the target pool can garner additional rewards surpassing those obtained in PAW.

Furthermore, we elucidate the possibility of two mining pools employing the BM-PAW attack against one another. To address the third question, we delve into the analysis of the Nash equilibrium in a game involving two pools engaging in BM-PAW. Our findings indicate that the BM-PAW attacker can circumvent the "miner's dilemma", where the outcome is traditionally dictated by the pool size, with the larger pool emerging victorious. Notably, under the Nash equilibrium, one pool can meet the criteria for victory and achieve higher profits compared to honest mining, thereby overcoming the "miner's dilemma".

Finally, we deliberate upon practical countermeasures to mitigate the impact of advanced attacks involving bribe money, thereby fostering innovative ideas for future research directions.

1.2   Related Work

BWH Attacks. The attacker can adopt the BWH attack to destroy reward for the victim pool [9]. He divides the mining power into innocent mining pool and infiltration mining pool. When the infiltration pool finds a valid block (full proof of work, FPoW), he withholds it and continues to submit other shares (partial proof of work, PPoW) to obtain the share reward. The victim mining pool will never get reward from the attacker's infiltration mining. Hence, the victim pool will suffer a loss. Other miners, including the attacker's innocent pool, will gain more reward for the loss of the victim pool. [12] indicates that when the attacker splits his mining power properly, BWH attack is more profitable than selfish mining. However, when multiple independent pools adopt BWH attack against each other, they will encounter the "miner's dilemma" [13].

FAW Attacks. The FAW attack extends BWH with forks [10]. In brief, the BWH attacker will discard the discovered FPoW, while the FAW attacker will reserve the FPoW. When other miners (not in the victim pool) find a valid blocks, the attacker will release and submit the previously reserved FPoW and generate a fork. An FAW attacker can get more reward than in BWH and avoid miner's dilemma. When the attacker's FPoW is not selected as the main chain, FAW degenerates into BWH. [11] combines mining power adjustment strategy with FAW attack, allowing the attacker to adjust mining power dynamically between innocent mining and infiltration mining. Furthermore, [14] proposes FWAP where the mining pool pays the attacker for withholding a fork, which brings higher reward for both the attacker and the paying pool.

Bribery Attacks. The bribery attack can increase the probability of the attacker's branch being selected as the main chain in forking competition [15], which is always considered to combine with other attacks with forks [16,17]. Bribery attack can be launched in a less visible way [18]. [11] combines bribery attack with selfish mining, which indicates that BSM could bring 10% extra rewards to the attacker than honest mining. However, BSM may cause the "venal miner's dilemma". [19] proposes an optimal BSM to avoid the "venal miner's dilemma", where the miner is considered perfectly rational. [20] proposes a mixed scenario where the attacker alternates his strategies between BWH, FAW, and PAW. The mixed strategy is proved to be much higher in revenue than honest mining.

2   Preliminaries

2.1   Mining Process

The issuance process of Bitcoin is facilitated by the Bitcoin system, which generates a predetermined quantity of Bitcoins as a reward for miners, thereby assigning the role of currency issuer to the miners. This process of creating a new block is commonly referred to as mining. All Bitcoin transactions must be bundled into blocks and subsequently recorded in the blockchain ledger. The miner who first identifies a nonce that satisfies the specified difficulty criteria is

eligible to receive the coinbase reward (also known as the block reward). The mining process serves as an incentive for miners to uphold the security of the blockchain. The total supply of Bitcoins is capped at 21 million. Initially, each miner who successfully publishes a block receives a coinbase reward of 50 Bitcoins, which undergoes a halving event every four years. It is anticipated that by 2104, the coinbase reward will become too small to be further subdivided, marking the completion of the issuance of all Bitcoins.

2.2   Forks

When multiple valid blocks are concurrently generated, a forking event occurs. An honest miner will designate the first received valid block as the header [21]. Subsequently, one of the branches will emerge victorious in the competition and ultimately become the main chain. A miner who successfully publishes a block on the main chain will be awarded the corresponding coinbase reward, whereas other miners involved in the forked branches will receive no reward. It is worth noting that forks can also be intentionally induced, such as through selfish mining or FAW attacks.

2.3   Mining Pool

As the investment in mining power for PoW-based blockchain continues to escalate, the likelihood of an individual miner discovering a valid block diminishes significantly. Consequently, miners increasingly tend to join organizations known as mining pools. Typically, a mining pool comprises a pool manager and numerous peer miners who collaborate to solve the same cryptographic puzzle. Upon successfully generating a valid block, the mining pool's participants will divide the reward according to a predefined distribution protocol, such as Pay Per Share (PPS), Pay Per Last N Shares (PPLNS), or Pay Proportionally (PROP) [22], among others. In theoretical analysis, a miner's reward is directly proportional to their mining power. Therefore, by joining a mining pool, a miner can significantly mitigate the variability in profit. Currently, the majority of blocks in Bitcoin are generated by mining pools, including AntPool [23], Poolin [24], and F2Pool [25].

3   Threat Model and Assumption

3.1   Threat Model

An attacker may manifest as an individual miner or as a mining pool comprising multiple miners. Honest miners, motivated by profit maximization, are inclined to adopt optimal mining strategies to augment their earnings without initiating any mining attacks. Furthermore, the attacker has the capability to establish multiple identities through Sybil attacks and subsequently participate in various open mining pools utilizing distinct accounts and identifiers. Concurrently,

the attacker's mining power is constrained to prevent the execution of a 51% attack. The attacker can allocate their mining power across different strategies, including honest mining within an innocent mining pool (behaving as an honest miner), infiltration mining within other pools, or engaging in other mining attack methodologies. More precisely, within our proposed BM-PAW model, the attacker allocates their mining power to both innocent mining pools and infiltration mining pools. Ultimately, the attacker can create Sybil nodes within the network to prioritize the dissemination of their generated blocks, thereby enhancing the likelihood of their branch being selected as the main chain in the event of a fork.

3.2   Assumptions

To facilitate our analysis, we adopt a series of plausible assumptions that align with those employed in the study of other mining attacks, such as selfish mining [5], greedy mining [26], and bribery stubborn mining [27].

- Normalization of Mining Power: We normalize the total mining power of the system to unity. Within this framework, the attacker's normalized mining power is bounded between 0 and 0.5, excluding both endpoints. This constraint is intended to preclude the possibility of a 51% attack.
- Profit-Driven Miner Behavior: Miners are motivated by profit maximization. An honest miner may adopt what they perceive as the optimal mining strategy to enhance their earnings but refrain from initiating mining attacks. This assumption is grounded in the recognition that miners are honest but inherently profit-driven. In scenarios where the blockchain forks, and the lengths of the competing branches are equivalent, miners have the discretion to select any branch.
- Absence of Unintentional Forks: We assume that unintentional forks are absent in the PoW-based blockchain system. This presumption is justified by the negligible probability of such events occurring, estimated to be approximately 0.41% [28]. In conjunction with Assumption 1, the expected reward for a miner is equivalent to their probability of discovering a valid block in each round. Given the exponential distribution of block discovery times [29], where the mean is inversely proportional to a miner's mining power, the probability of a miner finding a valid block corresponds to their normalized mining power.
- Normalization of Block Reward: We normalize the block reward (coin-base reward) to unity, rather than the current Bitcoin reward of 3.125 BTCs. In our analysis, miners' rewards are both expected and normalized.
- Reward Distribution in Mining Pools: Upon discovering an FPoW, a pool manager will propagate the valid block to obtain the block reward and subsequently distribute it among pool miners based on the number of submitted shares (PPoW and FPoW) in each round.
- Bribery in Forking Competition: Certain miners may offer bribe money to the target to increase the likelihood of their FPoW being selected as the main

chain in a forking competition. This assumption acknowledges the potential for strategic bribery in the context of blockchain forking.

4   One-pool: BM-PAW

4.1   Overview

We introduce a novel mining attack strategy that leverages bribe money as a strategic mechanism. Specifically, the attacker offers bribe money to target miners in order to enhance the probability of their FPoW being selected as the main chain in a forking competition. By integrating this bribe money strategy with PAW attack, we derive a unique mining strategy termed BM-PAW. The fundamental principle underlying our innovative BM-PAW attacks is the utilization of monetary incentives to target miners for the purpose of maximizing profit. The attacker possesses the capability to dynamically allocate their mining power between honest mining and infiltration mining. Furthermore, in scenarios involving forking competitions, the attacker can employ additional monetary incentives to target miners.

4.2   Method

In comparison to the PAW attack, our one-pool BM-PAW framework adopts several additional parameters, which are intorduced in Appendix A.1. Specifically, BM-PAW comprises four distinct participant types: the attacker, the victim pool, the target pool, and other miners. We denote the total mining power of the target pool, which consists of miners pre-bribed by the attacker, as η. Notably, the mining power of other miners, denoted as δ, is calculated as $1 - \alpha - \beta - \eta$, where α, β, and η represent the mining power of the attacker, the victim pool, and the target pool, respectively. It is important to clarify that the total mining power of the victim pool (β) excludes the attacker's infiltration mining power. The Markov state transition diagram of BM-PAW attack is shown in Figure 1.

Prior to power adjustment (Case 5), the attacker allocates $(1 - r_1)\alpha$ mining power for honest mining and $r_1\alpha$ for infiltration mining. Post-adjustment, the attacker employs $(1 - r_2)\alpha$ and $r_2\alpha$ for honest and infiltration mining, respectively. The parameter c is associated with the PoW-based blockchain network topology and the attacker's network capabilities, and its value can be derived using the methodology outlined in the FAW attack.

It is crucial to recognize that, due to the availability of bribe money to any miner selecting the attacker's FPoW, our BM-PAW model may involve multiple targets. In this analysis, η represents a single target, as we focus on optimizing the strategy for one target. The involvement of additional targets is contingent upon the bribe money offered, denoted as ε_1 and ε_2, with a greater amount of bribe money attracting more targets.

The relationship between c and γ varies based on whether the target accepts or denies the bribe money. Specifically, when the target accepts the bribe
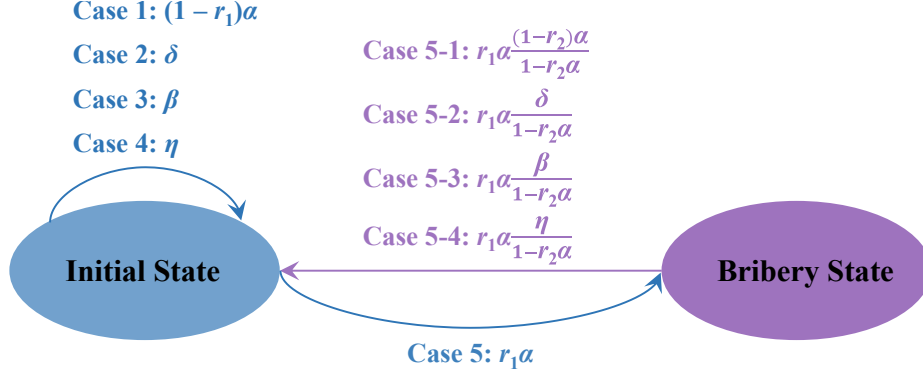
Fig. 1: The Markov state transition diagram of BM-PAW attack.

(Cases 5-2 and 5-4), the relationship is given by $c_{Case\ 5\text{-}2} = \frac{(1-r_2)\alpha+\eta+\beta+\gamma\delta}{1-r_2\alpha}$ and $c_{Case\ 5\text{-}4} = 1$, respectively. Conversely, if the target denies the bribe (Cases 5-2' and 5-4'), the relationships are defined as $c_{Case\ 5\text{-}2'} = \frac{(1-r_2)\alpha+\beta+\gamma(\delta+\eta)}{1-r_2\alpha}$ and $c_{Case\ 5\text{-}4'} = \frac{(1-r_2)\alpha+\beta+\gamma\delta}{1-r_2\alpha}$.

The distinction between bribe money ε_1 in Case 5-2 and ε_2 in Case 5-4 arises due to the target's decision to accept or deny the bribe, which is influenced by the specific branch in question. For instance, in Case 5-2, the target may accept even a minimal positive proportion of reward (ε_1). However, in Case 5-4, the target will only accept the bribe if the amount offered exceeds the potential reward loss incurred by accepting it.

In the context of the PAW attack, we contemplate a scenario where the adversary initially partitions their mining power into two components: innocent mining and infiltration mining, within a single victim pool. The adversary possesses the capability to modulate the allocation ratio of their mining power upon discovering a valid FPoW through infiltration mining. A notable distinction between the BM-PAW attack and the traditional PAW attack lies in the fact that the adversary in the BM-PAW attack offers bribe money to the target miners, thereby enhancing the likelihood of their FPoW being selected as the main chain in a forking competition. To elaborate further, there exist five conceivable scenarios when a valid block, specifically an FPoW, is discovered:

- **Case 1.** Found by the attacker's innocent pool. The attacker will immediately propagate it and obtain the block reward (coin-base reward) in this case.
- **Case 2.** Found by other miners who are none of attacker, target pool and victim pool. The attacker will accept it and continue mining the next block. He cannot get any reward in this case.
- **Case 3.** Found by the victim pool which is none of the attacker's infiltration mining power. The attacker will accept it and continue mining the next block. He obtains the share reward from this pool in this case.

- **Case 4.** Found by the target pool. This case is similar to Case 2, in which the attacker will accept it and continue mining the next block. He earns nothing in this case.
- **Case 5.** Found by the attacker's infiltration pool. The attacker will withhold the block and re-adjust his mining power. Meanwhile, there are further four subcases when another valid block/FPoW is found:
    - **Case 5-1.** Found by the attacker's innocent pool. The attacker will discard the withheld FPoW and propagate the new one. He obtains the block reward in this case.
    - **Case 5-2.** Found by other miners who are none of attacker, target pool and victim pool. The attacker will swiftly submit the previously withheld FPoW to the manager of the victim pool. A blockchain fork occurs when the manager distributes their own FPoW across the network. Simultaneously, the attacker attempts to entice the target miners to mine on the attacker's FPoW by offering an incentive. If the target decides to accept this enticement and mine on the attacker's FPoW, they will receive a bribe paid by the attacker. Alternatively, the target may adopt an honest mining strategy, akin to other miners. It is noteworthy that the target will opt to accept the bribe even if the attacker allocates an extremely small positive proportion of the reward, denoted as ε_1. In this instance, the attacker obtains the forking reward. It is important to acknowledge that the nature of the forking reward differs depending on whether the target accepts or declines the bribe, which will be discussed in greater detail subsequently.
    - **Case 5-3.** Found by the victim pool which is none of the attacker's infiltration mining power. The attacker will accept it and discard the withheld FPoW. He earns the share reward from this pool in this case.
    - **Case 5-4.** Found by the target pool. The attacker will immediately submit the withheld FPoW to the victim pool manager. Meanwhile, the attacker lures the target to discard his FPoW. The target will get the bribe money paid by the attacker if he chooses to accept the lure and mine on attacker's FPoW. Otherwise, he will propagate his FPoW and forking occurs. The target may accept bribe money only when the bribe money paid by the attacker is greater than the reward loss suffered by the target in accepting the bribe money. The attacker gets the share reward (the target accepting the bribe money) or forking reward (the target denying the bribe money) in this case.

In general, the mining strategy employed in the BM-PAW attack shares similarities with the PAW attack. However, a key distinction lies in the introduction of an additional participant class in the BM-PAW attack: the target miners, which complicates the strategic scenarios. Specifically, we introduce Case 4 during the phase preceding the adjustment of mining power. In this case, if a valid block is discovered by the target pool, the attacker will accept it and proceed to mine the subsequent block. Furthermore, we revise Case 5-2 and introduce Case 5-4 during the phase following the reallocation of mining power. During the
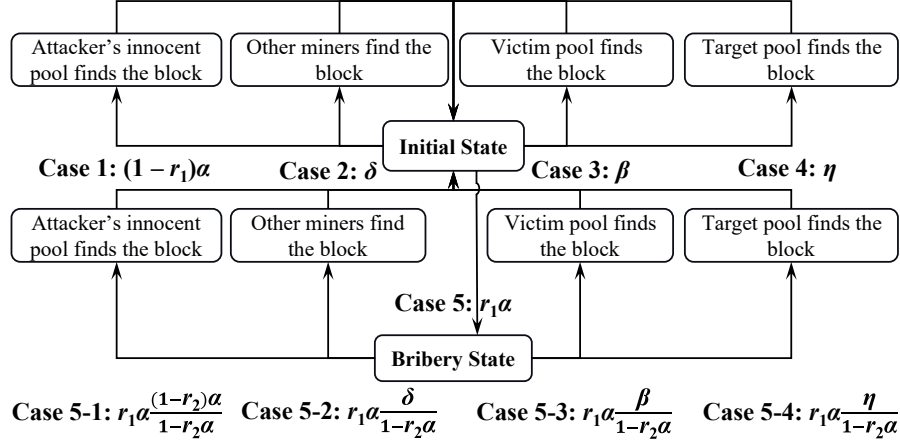
Fig. 2: The workflow of the overall BM-PAW attack.

forking competition stage, the attacker attempts to persuade the target miners to mine on the attacker's FPoW. In Case 5-2, where the fork occurs between the attacker's FPoW and an FPoW from other miners, the target will accept the bribe even if the attacker offers only an extremely small positive proportion of the reward, denoted as ε_1. Conversely, in Case 5-4, where the fork is between the attacker's FPoW and the target's FPoW, the target may only accept the bribe if the proportion of the reward, denoted as ε_2, is sufficiently large. Additionally, we will demonstrate that the bribe serves as an incentive for the attacker to adjust their attack parameters (r_1, r_2, ε_1 and ε_1) to maximize their profits. The workflow of the overall BM-PAW attack can be found in Figure 2.

4.3   Reward Analysis

Before analysis, we first define the additional entities in Appendix A.2.

Based on a comprehensive analysis of each aforementioned scenario, we can deduce that the probability of the attacker falling into Case 1 is $(1 - r_1)\alpha$; the probability for Case 2 is δ; the probability for Case 3 is β; the probability for Case 4 is η; and the probability for Case 5, prior to mining power adjustment, is $r_1\alpha$. It is noteworthy that the sum of these probabilities, as expected, totals to 1.

Subsequently, after adjusting the mining power, the occurrence probabilities for scenarios 5-1, 5-2, 5-3, and 5-4 are respectively calculated as $r_1\alpha \cdot \frac{(1-r_2)\alpha}{1-r_2\alpha}$, $r_1\alpha \cdot \frac{\delta}{1-r_2\alpha}$, $r_1\alpha \cdot \frac{\beta}{1-r_2\alpha}$, and $r_1\alpha \cdot \frac{\eta}{1-r_2\alpha}$. It is important to observe that the cumulative probability of these four scenarios equals $1 - r_2\alpha$, given that infiltration mining ceases to propagate any FPoW post-adjustment of mining power.

When the target accepts the bribe money, we can derive the reward of a BM-PAW attacker $R_a^{BM-PAW'}$ as follows:

$$R_a^{(BM-PAW)}(r_1, r_2) = R_a^{IMR} + R_a^{SR} + R_a^{FR} - R_a^{BM} \tag{1}$$
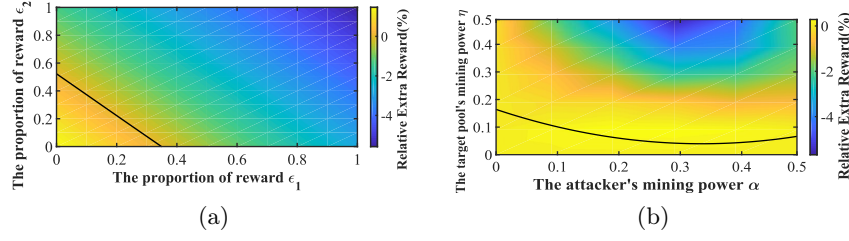
Fig. 3: The attacker's relative extra reward $RER_a^{BM-PAW,PAW}$ in different scenarios.

We can get the optimal infiltration mining power r_1, r_2 and $\bar{r}$ respectively since the proportion of reward as bribe money ε_1 and ε_2 are pre-defined. Therefore, the attacker can adjust his infiltration mining power optimally to maximize his profit.

Clearly, BM-PAW downgrades to PAW when the target denies the bribe money. Therefore, we can further derive the reward of a PAW attacker R_a^{PAW} as follows:

$$R_a^{PAW}(r_1, r_2) = R_a^{IMR} + R_a^{SR} + R_a^{FR'} \tag{2}$$

The attacker's reward is derived by bribe money R_a^{BM}, innocent mining reward R_a^{IMR}, share reward R_a^{SR} and forking reward R_a^{FR} (the target accepting the bribe money) or $R_a^{FR'}$ (the target denying the bribe money). More specifically, we have two cases for innocent mining reward: Case 1 and Case 5-1. The attacker's innocent mining reward R_a^{IMR} is $(1-r_1)\alpha + r_1\alpha \cdot \frac{(1-r_2)\alpha}{1-r_2\alpha}$. The share reward is related to two cases: Case 3 and Case 5-3. The attacker's share reward R_a^{SR} is $\beta \cdot \frac{r_1\alpha}{r_1\alpha+\beta} + r_1\alpha \cdot \frac{\beta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$. For forking reward, we have two cases: Case 5-2 and Case 5-4. The attacker's forking reward R_a^{FR} is $c_{Case\ 5-2}r_1\alpha \cdot \frac{\delta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-2 and $c_{Case\ 5-4}r_1\alpha \cdot \frac{\eta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-4 when the target chooses to accept the bribe money. Furthermore, the attacker's bribe money R_a^{BM} consists of two parts, namely $\varepsilon_1 c_{Case\ 5-2}r_1\alpha \cdot \frac{\delta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-2 and $\varepsilon_2 c_{Case\ 5-4}r_1\alpha \cdot \frac{\eta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-4. Once the target denies the bribe money, the attacker's forking reward $R_a^{FR'}$ is $c_{Case\ 5-2'}r_1\alpha \cdot \frac{\delta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-2 and $c_{Case\ 5-4'}r_1\alpha \cdot \frac{\eta}{1-r_2\alpha} \cdot \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta}$ in Case 5-4. In summary, R_a^{BM-PAW} is derived by separating the attacker's reward into R_a^{IMR}, R_a^{SR}, R_a^{FR}, and R_a^{BM} while R_a^{PAW} is related to R_a^{IMR}, R_a^{SR} and $R_a^{FR'}$. Therefore, we can derive the reward of a BM-PAW attacker R_a^{BM-PAW} in Equation (1) and the reward of a PAW attacker R_a^{PAW} in Equation (2).

Then, we can derive the attacker's extra reward R_a as follows:

$$R_a(r_1, r_2) = R_a^{BM-PAW}(r_1, r_2) - R_a^{PAW}(r_1, r_2) = R_a^{FR} - R_a^{BM} - R_a^{FR'}$$
$$= r_1\alpha \left(\begin{array}{l} ((1-\varepsilon_1)c_{Case\ 5-2} - c_{Case\ 5-2'})\frac{\delta}{1-r_2\alpha} \\ + ((1-\varepsilon_2)c_{Case\ 5-4} - c_{Case\ 5-4'})\frac{\eta}{1-r_2\alpha} \end{array} \right) \frac{\bar{r}\alpha}{\bar{r}\alpha+\beta} \tag{3}$$

Table 1: The attacker's optimal infiltration mining power $\hat{r}_1$ and $\hat{r}_2$ in BM-PAW in different scenarios. The values $\hat{r}_1(\hat{r}_2)$, $\hat{r}_1$, $\hat{r}_2$ indicate the optimal infiltration mining power before and after the mining power adjusting respectively.

β	$\alpha=0.1$	$\alpha=0.2$	$\alpha=0.3$	$\alpha=0.4$
0.1	0.1404(0.9985)	0.1222(0.6787)	0.1254(0.4903)	0.1372(0.3938)
0.2	0.3039(0.9996)	0.2844(0.9993)	0.2928(0.7998)	0.3271(0.6334)
0.3	0.2745(0.6771)	0.3079(0.3098)	0.3691(0.1313)	0.4791(0.0002)

How to adjust the attacker's infiltration mining power that could maximize his rewards? Based on the attacker's system reward in BM-PAW, we formalize the optimal strategy of mining power adjusting by finding the best proportion of attacker's mining power ($\hat{r}_1$ and $\hat{r}_2$) to maximize his expected reward $(R_a^{BM-PAW'}(r_1,r_2))$:

$$
\begin{aligned}
&\arg\max_{r_1,r_2} R_a^{BM-PAW'}\left(r_1,\ r_2\right), \\
&s.t.\ \ 0 \le r_1 \le 1,\ 0 \le r_2 \le 1.
\end{aligned}
\tag{4}
$$

We can use Lagrange multipliers to solve Equation (3). Specifically, we rewrite Equation (4) as follows:

$$
\begin{aligned}
&\arg\min_{r_1,r_2} -R_a^{BM-PAW'}\left(r_1,\ r_2\right), \\
s.t.\ \ &g_1\left(r_1,r_2\right) = -r_1 \le 0; \\
&g_2\left(r_1,r_2\right) = r_1 - 1 \le 0; \\
&g_3\left(r_1,r_2\right) = -r_2 \le 0; \\
&g_4\left(r_1,r_2\right) = r_2 - 1 \le 0;
\end{aligned}
\tag{5}
$$

As expected, the objective function $-R_a^{BM-PAW'}(r_1,r_2)$ is a convex function when $r_1, r_1 \in [0,1]$ as the Hessian matrix is positive definite. Hence, we can find the optimal $\hat{r}_1$ and $\hat{r}_2$ by solving the KKT conditions, which are shown in Table 1.

Meanwhile, we can derive the following theorem with the optimal $\hat{r}_1$ and $\hat{r}_2$. Detailed proofs of Theorems 1 and 2 are provided in [30].

Theorem 1. *A BM-PAW attacker can always earn more reward than honest mining, and the reward of a BM-PAW attacker has a lower bound defined by the reward from an FAW attack.*

Theorem 2. *When ε_1 and ε_2 satisfy $\delta c_{Case\ 5\text{-}2}\cdot\varepsilon_1+\eta c_{Case\ 5\text{-}4}\cdot\varepsilon_2 < \delta(c_{Case\ 5\text{-}2}-c_{Case\ 5\text{-}2'}) + \eta\left(c_{Case\ 5\text{-}4} - c_{Case\ 5\text{-}4'}\right)$, a BM-PAW attacker can always obtain more reward than a PAW attacker.*
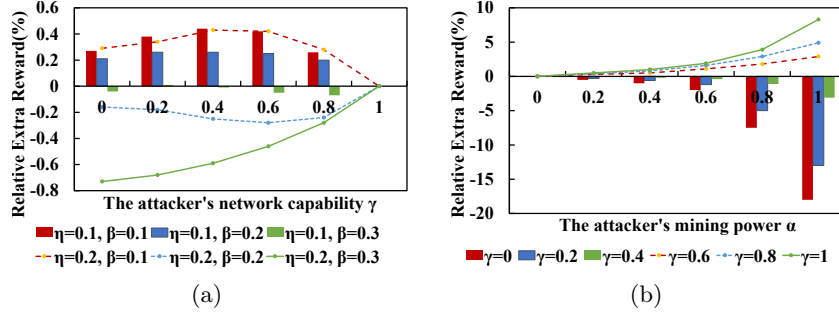
Fig. 4: The attacker's relative extra reward $RER_a^{BM-PAW,PAW}$ in different parameters.

4.4   Implementation and Evaluation

We adopt expected relative extra reward (RER) to evaluate BM-PAW attack, which can be expressed as $RER_\tau^{S_1,S_2} = \frac{R_\tau^{S_1} - R_\tau^{S_2}}{R_\tau^{S_2}}$, where τ represents the participant role (i.e., the attacker (a), the target (t) and etc.), and S indicates different strategies (i.e., BM-PAW, PAW, etc.). We implement a Monte Carlo simulator in MATLAB to verify the accuracy of our theoretical analysis of BM-PAW attack. We run it over 10^9 rounds to derive a BM-PAW attacker's reward when $\alpha = 0.2$, $\beta = \{0.1, 0.2, 0.3\}$ and $\eta = \{0.1, 0.2\}$. Then we calculate the attacker's RER during the process.

First, consider a specific case: the attacker has mining power $\alpha = 0.2$, the victim pool has mining power $\beta = 0.2$, the target pool has mining power $\eta = 0.2$, and the ratio of other miners that select the attacker's FPoW $\gamma = 0.5$. $RER_a^{BM-PAW,PAW}$ with varying ε_1 and ε_2 is depicted in Fig. 3a. The left side of the solid line indicates that the BM-PAW attacker can obtain more reward than in PAW. The BM-PAW attacker's RER increases when the proportion of reward ε_1 and ε_2 decrease, since the bribe money is determined by ε_1 and ε_2. More specifically, the smaller ε_1 and ε_2 are, the lower the bribe money is, which is consistent with our reward analysis.

Moreover, considering $\beta = 0.2$, the minimum ε_1 and ε_2 when the target pool is willing to accept the bribe money, $RER_a^{BM-PAW,PAW}$ with varying α and η is shown in Fig. 3b. The lower part of the solid line indicates that BM-PAW is the dominant strategy compared with PAW, which can bring higher profit for the BM-PAW attacker. In addition, the attacker's RER increases when the victim pool's mining power decreases, since the attacker can get more share reward from target pool. Meanwhile, the attacker has the motivation to launch BM-PAW attack when the target pool possesses little mining power regardless of his own mining power, which is more profitable.

Furthermore, we take into account $\alpha = 0.2$, $\eta = \{0.1, 0.2\}$, $\beta = \{0.1, 0.2, 0.3\}$, the minimum ε_1 and ε_2, $RER_a^{BM-PAW,PAW}$ with varying γ is shown in Fig. 4a.

The attacker's RER is related to his network capability. He can earn higher profit when the victim pool infiltrated by the attacker has less mining power, regardless of his network capability, since the attacker can earn more share reward from target pool. Therefore, the pool with lower mining power is more vulnerable to attack.

Finally, Fig. 4b represents $RER_a^{BM-PAW,PAW}$ with varying α, and constant $\beta = 0.2$, $\eta = 0.2$, the minimum ε_1 and ε_2, $\gamma = \{0 : 0.1 : 1\}$, which indicates that the higher attacker's network capability cannot always obtain higher RER. The reason is that the attacker's network capability will affect both BM-PAW and PAW simultaneously.

5   Bribe Money Pricing

5.1   Overview

We assume that there exists a secret protocol with the bribe money ratio ε_1 in Case 5-2 as well as ε_2 in Case 5-4 to launch the BM-PAW attack between the BM-PAW attacker and the target pool. Here, we focus on analyzing the constraint condition of ε_1 and ε_2 in order to bring about the BM-PAW attack effective and profitable. We let R_t^{BM-PAW} be the target pool's total reward in BM-PAW (i.e., the target accepting the bribe money) and R_t^{PAW} be the target pool's total reward in PAW (i.e., the target denying the bribe money) respectively. When the attacker cannot afford enough bribe money to motivate the target pool to accept it, the BM-PAW attack downgrades to the PAW attack. Meanwhile, the attacker's reward should be improved in the BM-PAW attack as well after paying bribe money to the target. Otherwise, it is more profitable for attacker to exploit the PAW attack. We can get the reward of the target pool in the PAW attack denoted by R_t^{PAW} which will be adopted as the baseline of the bribe money ratio ε_1 and ε_2 with the same parameters. What is the most significant is that the minimum bribe money must be sufficient to guarantee the reward of the target in BM-PAW is greater than in PAW and the maximum bribe money must guarantee the reward of the attacker in BM-PAW is larger than in PAW, namely $R_t^{BM-PAW} > R_t^{PAW}$ and $R_a^{BM-PAW} > R_a^{PAW}$.

5.2   Reward Analysis

First, when the target pool accepts the bribe money, we can obtain the target pool's reward R_t^{BM-PAW} in the BM-PAW attack as follows:

$$
\begin{aligned}
R_t^{BM-PAW}\left(r_1,\ r_2\right) = {} & \eta + r_1\alpha \left(\frac{\delta}{1 - r_2\alpha} + \frac{\eta}{1 - r_2\alpha}\right) \frac{\eta}{1 - r_2\alpha} \\
& + r_1\alpha \left(\varepsilon_1 c_{Case\ 5\text{-}2} \cdot \frac{\delta}{1 - r_2\alpha} + \varepsilon_2 c_{Case\ 5\text{-}4} \cdot \frac{\eta}{1 - r_2\alpha}\right) \frac{\overline{r}\alpha}{\overline{r}\alpha + \beta}
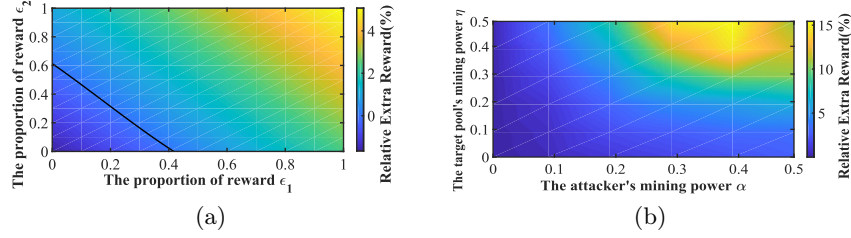\end{aligned}
\tag{6}
$$

Fig. 5: The target pool's relative extra reward $RER_t^{BM-PAW,PAW}$ in different scenarios.

Furthermore, when the target pool denies the bribe money, we derive the target pool's reward R_t^{PAW} in the PAW attack as follows:

$$R_t^{PAW}(r_1,\ r_2) = \eta + r_1\alpha \cdot \frac{\delta}{1-r_2\alpha} \cdot \frac{\eta}{1-r_2\alpha}$$
$$+ r_1\alpha \cdot \frac{\eta}{1-r_2\alpha}\left(1 - c_{Case\ 5\text{-}4'} + \frac{\eta}{1-r_2\alpha}\right) \tag{7}$$

Therefore, we can get the target pool's extra reward R_t as follows:

$$R_t(r_1,\ r_2) = R_t^{BM-PAW}(r_1,\ r_2) - R_t^{PAW}(r_1,\ r_2)$$

$$= r_1\alpha\left(\varepsilon_1 c_{Case\ 5\text{-}2} \cdot \frac{\delta}{1-r_2\alpha} + \varepsilon_2 c_{Case\ 5\text{-}4} \cdot \frac{\eta}{1-r_2\alpha}\right)\frac{\bar{r}\alpha}{\bar{r}\alpha + \beta} \tag{8}$$

$$- r_1\alpha \cdot \frac{\eta}{1-r_2\alpha}\left(1 - c_{Case\ 5\text{-}4'}\right)$$

How to choose the proper bribe money to achieve incentive compatibility between the attacker and the target pool? Below, we present Theorem 3 to address the aforementioned questions. Detailed proofs of Theorems 3 and 4 are provided in [30].

Theorem 3. *When ε_1 and ε_2 satisfy $\delta c_{Case\ 5\text{-}2} \cdot \varepsilon_1 + \eta c_{Case\ 5\text{-}4} \cdot \varepsilon_2 > \eta(1 - c_{Case\ 5\text{-}4'})\frac{\bar{r}\alpha+\beta}{\bar{r}\alpha}$, the target pool can always get higher reward in the BM-PAW attack than in the PAW attack.*

Theorem 4. *Once launching BM-PAW, both the BM-PAW attacker and the target pool can get higher reward than in the PAW attack when the attacker pays proper bribe money and the target accepts it.*

The result of Theorem 4 guarantees that a rational attacker is willing to launch BM-PAW attack and a greedy target pool has motivation to accept the bribe money and join it. Furthermore, once the attacker decides to execute the BM-PAW attack with pre-determined ε_1 and ε_2, it is motivated for him to adjust the optimal attack parameters (i.e., r_1 and r_2) to maximize his extra reward. Notice that a PAW attacker adopts a similar approach to determine the optimal r_1 and r_2.
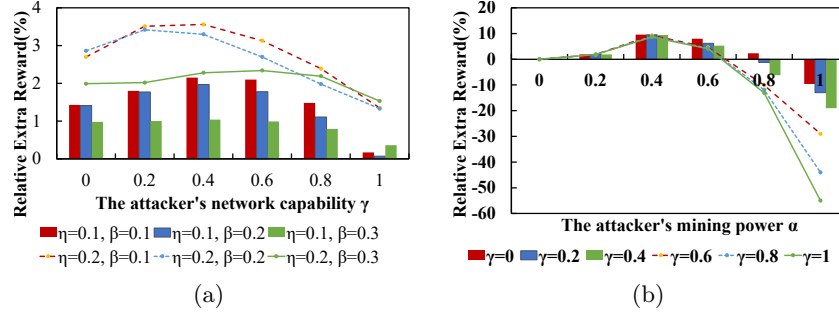
Fig. 6: The target pool's relative extra reward $RER_t^{BM-PAW,PAW}$ in different parameters.

5.3   Implementation and Evaluation

We further use a Monte Carlo simulator verify our analysis. We run it over 10^9 rounds when $\alpha = 0.2$, $\eta = \{0.1, 0.2, 0.3\}$ and $\beta = \{0.1, 0.2, 0.3\}$. Then we calculate the target pool's RER during the process.

First, Fig. 5a shows $RER_t^{BM-PAW,PAW}$ with varying ε_1 and ε_2, and constant $\alpha = 0.2$, $\beta = 0.2$, $\eta = 0.2$ and $\gamma = 0.5$. The right side of the solid line indicates that the target pool accepting the bribe money can obtain more reward than denying. The target's RER increases with ε_1 and ε_2 increasing, since the target will get higher reward with the attacker paying more bribe money. Therefore, accepting the bribe money is always the optimal strategy for the target when the attacker offers proper bribe money.

Moreover, Fig. 5b represents $RER_t^{BM-PAW,PAW}$ with varying α and η, and constant $\beta = 0.2$, $\eta = 0.2$, $\gamma = 0.5$, and the maximum ε_1 and ε_2. The target pool can always get more reward when the attacker pays the maximum bribe money. Hence, accepting the bribe money is the optimal strategy for the target, regardless of the mining power he possesses.

Furthermore, considering $\alpha = 0.2$, $\eta = \{0.1, 0.2\}$, $\beta = \{0.1, 0.2, 0.3\}$, the maximum ε_1 and ε_2, Fig. 6a shows $RER_t^{BM-PAW,PAW}$ with varying γ, which indicates the target has the incentive to accept the bribe money for most cases. Similarly, the target's RER increases when the victim pool's mining power decreases, since the target can get more bribe money from the attacker's share reward.

Finally, Fig. 6b depicts $RER_t^{BM-PAW,PAW}$ with varying α, and constant $\beta = 0.2$, $\eta = 0.2$, the maximum ε_1 and ε_2, and $\gamma = \{0 : 0.1 : 1\}$. We derive that the higher attacker's network capability cannot always obtain higher RER for the target since both BM-PAW and PAW are determined by the attacker's network capability simultaneously.

Table 2: Results of a BM-PAW game with varying $\alpha^{[2]}$ and c when $\alpha^{[1]} = 0.2$. The left side shows the RER of Pool_1, and the right side shows the RER of Pool_2.

$\alpha^{[1]}$	$c = 0.2$	$c = 0.6$	$c = 1$	$\alpha^{[2]}$	$c = 0.2$	$c = 0.6$	$c = 1$
0.1	0.9810	0.9982	1.0155	0.1	-0.4952	0.4995	-0.5038
0.2	-0.0177	-0.0089	0	0.2	0.01808	0.0090	0
0.3	-0.3491	-0.3441	-0.3392	0.3	0.5364	0.5248	0.5132
0.4	-0.5163	-0.5134	-0.5104	0.4	1.0678	1.0550	1.0424

6   Two-pool: Miner's Dilemma

Based on the analyze of the BM-PAW attack, we find that two mining pools can also exploit the BM-PAW attack against each other. We demonstrate that two-pool BM-PAW game can avoid the "miner's dilemma", in which the single winner is determined by the pool size (i.e., the larger pool can win). We define the winning condition as obtaining an extra reward to analyze the two-pool BM-PAW attack game.

We consider a game involving Pool_1 and Pool_2 with mining power $\alpha^{[i]}(i \in \{1, 2\})$. The Pool_i will distribute the infiltration mining power either $f_1^{[i]} = r_1^{[i]}\alpha^{[i]}$ (before the mining power adjusting) or $f_2^{[i]} = r_2^{[i]}\alpha^{[i]}$ (after the mining power adjusting) in his opponent $\text{Pool}_{\neg i}$, where $\neg i = 3 - i$ and $i \in \{1, 2\}$. Therefore, we further define the additional parameters in Appendix A.3.

To calculate $R_a^{[i]}$, we introduce the possible cases (which are parameterized by Pool_i) when a valid block (FPoW) is found in a two-pool BM-PAW game, which can be found in Appendix B.

In a two-pool BM-PAW game, the Pool_i's reward $R_a^{[i]}$ is derived from bribe money, innocent mining reward, share reward and forking reward.

What equilibrium will the BM-PAW game of different types of participants eventually reach? To answer the above question, we quantitatively analyze the reward in a two-pool BM-PAW game under the Nash equilibrium point. To simplify our analysis, we assume $c_1^{[1]} = c_1^{[2]} = c$ and $c_2^{[1]} = c_2^{[2]} = c/2$, where $0 \le c \le 1$. Table 2 shows the results of a two-pool BM-PAW game with varying $\alpha^{[2]}$ and c when $\alpha^{[1]}$=0.2. We find that Pool_2 may get more reward when $\alpha^{[2]}$>0.2, which is determined by his network capability. However, when $\alpha^{[1]} < 0.2$, Pool_2 will always suffer a loss. For Pool_1, it still follows the above pattern. Therefore, we can derive that the winning condition is determined by the attacker's mining power in a two-pool BM-PAW game, which breaks the "miner's dilemma".

7   Dicussion

We propose three countermeasures to address the emerging threat posed by bribery attacks utilizing monetary incentives. Initially, upon the occurrence of a

blockchain fork, honest miners ought to prioritize and select FPoW they detect. As an illustrative example, if a miner detects transaction T^A prior to a fork event that subsequently introduces a branch containing both transactions T^A and T^B, the miner should expand the blockchain along the branch incorporating T^A. If all miners adhere to this mining strategy, the effectiveness of bribery attacks can be significantly mitigated. However, it is important to acknowledge the impracticality of this assumption due to miners' profit-oriented nature, which may prompt them to opt for an alternative branch containing T^B to maximize their rewards. Despite this limitation, it is noteworthy that as the number of miners adopting this strategy increases, the value of γ decreases, resulting in reduced rewards for the attacker and consequently lowering the success probability of their FPoW in achieving consensus.

Secondly, upon detecting a bribery attack, the victim may consider employing a counter-bribery strategy by offering additional monetary incentives to secure higher profits. Typically, any miner who secures a reward on the legitimate main chain, rather than on the attacker's forked branch, can adopt such a counter-bribery approach. It is crucial to note that the victim's expenditure on counter-bribery measures should not exceed the total value of the transaction T^A. In the event that the attacker prevails in the competition, the victim stands to lose the entire value of T^A. Consequently, the attacker must increase the amount of bribe money offered to the target, rendering the bribery attack economically unviable.

Thirdly, there exists the potential for dynamic shifts in the roles of individual miners or mining pools. Specifically, the identities of the attacker, the victim, and the target pool are subject to continuous change over time. A miner who currently benefits from short-term gains as an attacker may subsequently incur losses in the role of a victim. Consequently, if the immediate rewards derived from bribery money compromise the long-term profit potential, miners will lack the motivation to initiate BM-PAW or to accept bribe money.

8   Conclusion

We introduce a novel mining attack, termed BM-PAW, which augments the existing PAW attack by incorporating a bribery strategy. We reveal that the BM-PAW attack can offer higher rewards to both the attacker and the target mining pool compared to the traditional PAW attack. While our primary focus is on the PoW-based blockchain system, the BM-PAW attack has the potential to be adapted for use in other PoW-based cryptocurrency systems. Through equilibrium analysis in a two-pool BM-PAW game scenario, where the winning condition is contingent upon the attacker's mining power, we find that the BM-PAW attacker can evade the classic "miner's dilemma". We finally propose practical countermeasures to mitigate these novel bribery-based pool attacks, which may offer fresh insights and inspiration to researchers in the field.

Acknowledgments

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto (2008)
2. "Bitcoin", https://en.bitcoin.it/wiki/Proofofwork, last accessed 1 November 2024
3. "Bitinfocharts", https://bitinfocharts.com/comparison/bitcoin-hashrate.html/, last accessed 1 November 2024
4. Schrijvers, O., Bonneau, J., Boneh, D., Roughgarden, T.: Incentive compatibility of bitcoin mining pool reward functions. In: Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20. pp. 477–498. Springer (2017)
5. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM **61**(7), 95–102 (2018)
6. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 305–320. IEEE (2016)
7. Li, T., Wang, Z., Yang, G., Cui, Y., Chen, Y., Yu, X.: Semi-selfish mining based on hidden markov decision process. International Journal of Intelligent Systems **36**(7), 3596–3612 (2021)
8. Li, T., Wang, Z., Chen, Y., Li, C., Jia, Y., Yang, Y.: Is semi-selfish mining available without being detected? International Journal of Intelligent Systems **37**(12), 10576–10597 (2022)
9. Courtois, N.T., Bahack, L.: On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718 (2014)
10. Kwon, Y., Kim, D., Son, Y., Vasserman, E., Kim, Y.: 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. pp. 195–209 (2017)
11. Gao, S., Li, Z., Peng, Z., Xiao, B.: Power adjusting and bribery racing: Novel mining attacks in the bitcoin system. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 833–850 (2019)
12. Luu, L., Saha, R., Parameshwaran, I., Saxena, P., Hobor, A.: On power splitting games in distributed computation: The case of bitcoin pooled mining. In: 2015 IEEE 28th Computer Security Foundations Symposium. pp. 397–411. IEEE (2015)
13. Eyal, I.: The miner's dilemma. In: 2015 IEEE symposium on security and privacy. pp. 89–103. IEEE (2015)
14. Yang, Z., Yin, C., Ke, J., Dinh, T.T.A., Zhou, J.: If you can't beat them, pay them: Bitcoin protection racket is profitable. In: Proceedings of the 38th Annual Computer Security Applications Conference. pp. 727–741 (2022)

15. Bonneau, J.: Why buy when you can rent? bribery attacks on bitcoin-style consensus. In: International Conference on Financial Cryptography and Data Security. pp. 19–26. Springer (2016)
16. Karame, G.O., Androulaki, E., Capkun, S.: Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM conference on Computer and communications security. pp. 906–917 (2012)
17. Zhang, M., Li, Y., Li, J., Kong, C., Deng, X.: Insightful mining equilibria. In: International Conference on Web and Internet Economics. pp. 21–37. Springer (2022)
18. McCorry, P., Hicks, A., Meiklejohn, S.: Smart contracts for bribing miners. In: Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22. pp. 3–18. Springer (2019)
19. Yang, G., Wang, Y., Wang, Z., Tian, Y., Yu, X., Li, S.: IPBSM: An optimal bribery selfish mining in the presence of intelligent and pure attackers. International Journal of Intelligent Systems **35**(11), 1735–1748 (2020)
20. Wang, Y., Yang, G., Li, T., Zhang, L., Wang, Y., Ke, L., Dou, Y., Li, S., Yu, X.: Optimal mixed block withholding attacks based on reinforcement learning. International Journal of Intelligent Systems **35**(12), 2032–2048 (2020)
21. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: IEEE P2P 2013 Proceedings. pp. 1–10. IEEE (2013)
22. Zolotavkin, Y., García, J., Rudolph, C.: Incentive compatibility of pay per last n shares in bitcoin mining pools. In: Decision and Game Theory for Security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017, Proceedings. pp. 21–39. Springer (2017)
23. "antpool", https://www.antpool.com/, last accessed 1 November 2024
24. "poolin", https://www.poolin.me/, last accessed 1 November 2024
25. Gencer, A.E., Basu, S., Eyal, I., Van Renesse, R., Sirer, E.G.: Decentralization in bitcoin and ethereum networks. In: Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22. pp. 439–457. Springer (2018)
26. Hu, J., Jiang, Z., Xu, C.: Greedy-mine: A profitable mining attack strategy in bitcoin-ng. International Journal of Intelligent Systems **2024**(1), 9998126 (2024)
27. Hu, J., Xu, C., Jiang, Z., Cao, J.: Novel bribery mining attacks in the bitcoin system and the bribery miner's dilemma. arXiv preprint arXiv:2305.07381 (2023)
28. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. pp. 3–16 (2016)
29. Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R.: Bitcoin-NG: A scalable blockchain protocol. In: 13th USENIX symposium on networked systems design and implementation (NSDI 16). pp. 45–59 (2016)
30. Hu, J., Chen, X., Yan, H., Ruan, N., BM-PAW: A Profitable Mining Attack in the PoW-based Blockchain System. arXiv preprint arXiv:2411.06187 (2024).

A   Symbol Definition

A.1

We adopt the following parameters to analyze the BM-PAW attack:

- α: The total mining power of the attacker;
- β: The total mining power of the victim pool;
- η: The total mining power of the target pool;
- δ: The mining power of other miners who are none of attacker, target pool and victim pool;
- r_1: The original infiltration mining power of the attacker as a proportion of α before power adjusting (Case 5) in each round;
- r_2: The reallocated infiltration mining power of the attacker as a proportion of α after power adjusting (Case 5) in each round;
- $\bar{r}$: The average infiltration mining power of the attacker as a proportion of α between a mining process;
- c: The probability of the attacker's FPoW will be selected as the main chain in Case 5-2 or Case 5-4.
- γ: The ratio of other miners that select the attacker's FPoW;
- ε_1: The fraction of reward as bribe money of the attacker willing to pay per block when the target pool chooses to accept bribe money in Case 5-2;
- ε_2: The proportion of reward as bribe money of the attacker willing to pay per block when the target pool chooses to accept bribe money in Case 5-4.

A.2

We define the following entities to analyze the reward in BM-PAW attack:

- R_a^{IMR}: The attacker's innocent mining reward;
- R_a^{SR}: The attacker's share reward;
- R_a^{FR}: The attacker's forking reward when the target accepts the bribe money;
- $R_a^{FR'}$: The attacker's forking reward when the target denies the bribe money;
- R_a^{BM}: The attacker's bribe money;
- $R_a^{BM-PAW'}$: The attacker's system reward in BM-PAW (excluding R_a^{BM});
- R_a^{PAW}: The attacker's total reward in PAW;
- R_a: The attacker's extra reward in BM-PAW compared with PAW;
- R_t^{BM-PAW}: The target pool's total reward in BM-PAW;
- R_t^{PAW}: The target pool's total reward in PAW;
- R_t: The target pool's extra reward in BM-PAW compared with PAW.

A.3

We define the following parameters to analyze the two-pool BM-PAW attack game:

- $\alpha^{[i]}$: The total mining power of Pool_i;
- $f_1^{[i]}$: The original infiltration mining power of Pool_i;
- $f_2^{[i]}$: The reallocated infiltration mining power of Pool_i;

- $c_1^{[i]}$: The probability of the Pool$_i$'s withheld FPoW is selected as the main chain in two-branch cases;
- $c_2^{[i]}$: The probability of the Pool$_i$'s withheld FPoW is selected as the main chain in three-branch cases;
- $R_a^{[i]}$: The reward of the Pool$_i$.

B   Possible Cases in Two-pool BM-PAW Game

- **Case 1.** Pool$_i$'s innocent mining finds an FPoW;
- **Case 2.** Pool$_i$'s infiltration mining first finds an FPoW (in Pool$_{\neg i}$) and then his innocent mining finds another FPoW;
- **Case 3.** Pool$_{\neg i}$'s infiltration mining first finds an FPoW (in Pool$_i$) and then Pool$_i$'s innocent mining finds another FPoW;
- **Case 4.** Pool$_1$'s infiltration mining (in Pool$_2$), Pool$_2$'s infiltration mining (in Pool$_1$) and Pool$_i$'s innocent mining find three FPoWs in order;
- **Case 5.** Pool$_2$'s infiltration mining (in Pool$_1$), Pool$_1$'s infiltration mining (in Pool$_2$) and Pool$_i$'s innocent mining find three FPoWs in order;
- **Case 6.** Pool$_{\neg i}$'s infiltration mining first finds an FPoW (in Pool$_i$) and then other miners (except Pool$_i$ and Pool$_{\neg i}$) find another FPoW;
- **Case 7.** Pool$_1$'s infiltration mining (in Pool$_2$), Pool$_2$'s infiltration mining (in Pool$_1$) and other miners find three FPoWs in order;
- **Case 8.** Pool$_2$'s infiltration mining (in Pool$_1$), Pool$_1$'s infiltration mining (in Pool$_2$) and other miners find three FPoWs in order;