Journal of Surveillance, Security and Safety

Original Article

Open Access

Resist the type of BWH attack: through introducing discount factor and withdrawal threshold into Bitcoin

Bizhong Wei[1,2,3], **Zihan Xiao**[1,2,3], **Fan Zhang**[1,2,3]

[1]School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China
[2]Guangxi Cooperative Innovation Center of cloud computing and Big Data, Guilin University of Electronic Technology, Guilin Guangxi 541004, Guangxi, China
[3]Guangxi Colleges and Universities Key Laboratory of cloud computing and complex systems, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China

Correspondence to: Prof. Bizhong Wei, School of Computer Science and Information Security, Guilin University of Electronic Technology, Qixing District, Jinji Ling No. 1, Guilin 541004, China. E-mail: wbz@guet.edu.cn

How to cite this article: Wei B, Xiao Z, Zhang F. Resist the type of BWH attack: through introducing discount factor and withdrawal threshold into Bitcoin. *J Surveill Secur Saf* 2023;3:35-46. https://dx.doi.org/10.20517/jsss.2023.07

Received: 5 Mar 2023 **First Decision:** 10 Apr 2023 **Revised:** 24 Apr 2023 **Accepted:** 27 Apr 2023 **Published:** 11 May 2023

Academic Editor: Mingwu Zhang **Copy Editor:** Yanbing Bai **Production Editor:** Yanbing Bai

Abstract

Aim: Since the emergence of the Block Withholding (BWH) attack, the prevailing approach in the environment has been to avoid attacking each other as a means of eliminating the threat posed by this attack. However, there is currently no effective and simple scheme to entirely prevent such attacks. To address this issue, this study proposes a novel blockchain model that combines the discount factor and withdrawal threshold to resist the risks associated with these attacks.

Methods: This paper provides an overview of blockchain models and the BWH attack. We constructed a network simulation model based on the physical logic of Bitcoin and introduced the discount factor and withdrawal threshold as new parameters to enhance the model's resistance to BWH attacks. We evaluated the effect of these parameters on the model's ability to defend against BWH attacks from the perspective of rewards.

Results: This paper presents a novel blockchain model that integrates discount factors and withdrawal thresholds and examines attacker behavior in this model from a rewards-based perspective by comparing different computational environments. Our experimental data indicate that this model has significant advantages in resisting BWH attacks.

Conclusion: The experimental results demonstrate that the proposed model is highly effective in resisting profit-driven BWH attacks, with a 98% chance of successfully resisting such attacks at a fixed computational power. This indicates that the proposed model can effectively eliminate the potential threat posed by BWH attacks.

Keywords: Blockchain, pool mining, Block Withholding attack

INTRODUCTION

Blockchain has become a popular platform technology for cryptocurrencies thanks to its encryption technologies of distributed ledger, Peer-to-Peer networking, and tamper-proof function. This has led to the emergence of various electronic currencies, such as Bitcoin[1] and Ethereum[2]. Due to its unique characteristics, blockchain technology has potential applications in access control[3], healthcare[4,5], metaverse[6], and data sharing and storage.

Blockchain uses a data structure called a block to store transaction information. Each block is unique and contains a hash value of the previous block, a *Merkle* root node containing a series of transactions, a *timestamp,* and other data that distinguish it from other blocks. In most cases, blockchain systems use Proof-of-Work (PoW) consensus algorithms, where participants called miners compete to create a new block through a process called mining. Mining involves solving complex mathematical problems to find the latest valid block that meets the system's requirements. The first miner to find the valid block is the winner and receives rewards, including a fixed coinbase reward of around 12.5 bitcoins[7] and some transaction fees.

Mining is a necessary process in blockchain systems, but it requires a significant amount of computational power. As a result, it is often inefficient for single miners with low computational power to compete in the mining process. To increase their chances of success, these miners often form groups called mining pools[8]. A mining pool *difficulty* is usually set lower than the system *difficulty*, allowing miners to find blocks more easily. When a miner in a mining pool finds a block that meets the *difficulty* of the mining pool, it is considered that the miner has made a contribution to the pool, and rewards are distributed to miners based on their contributions using various allocation methods such as proportional reward function, Pay-Per-Share (PPS) reward function, and Pay-Per-Last-N-Share (PPLNS) reward function. In this study, we use a proportional reward function.

While mining pools provide benefits to miners, such as stable earnings and shorter waiting times, they also bring new challenges, such as the *Block Withholding* (BWH) attack. In a BWH attack, an attacker injects part of its computational power into a target mining pool, submitting PoW that satisfies the *pool's difficulty* level while discarding PoW that satisfies the *system's difficulty* level. This allows the attacker to earn rewards from the target pool without contributing to it, resulting in losses for the pool and its members. Although mining pools generally agree not to launch BWH attacks, such consensus is not always effective in preventing these attacks, which remains profitable for attackers who can choose their target mining pool strategically to maximize their benefits[9]. This means that the current blockchain system is not fully protected against BWH attacks, and the attack can cause more miners to join the attacker, resulting in even greater losses for the attacked mining pool. Later on, we will describe the BWH attack mode in detail.

To address the threat of BWH attacks, we propose a new blockchain model called the DF model. This model introduces a discount factor and a withdrawal threshold into the traditional blockchain settlement model for the first time. The discount factor affects the block rewards and the withdrawal rewards, indicating the patience level of participants in game theory. A larger discount factor indicates greater patience on the part of the attacker, while the withdrawal threshold ensures that the attacker can only withdraw rewards from the target mining pool once they reach a certain amount. Once the attacker's rewards reach the withdrawal threshold, the discount factor applies to the rewards, weakening its penetration rewards. The DF model retains the basic logic of the traditional blockchain while ensuring that participants with a certain amount of computational power can maintain a stable reward. This makes it less rewarding for an attacker to launch an attack on a target mining pool using the best penetrating computing power than to mine honestly with its computing power. This effectively prevents profit-driven BWH attacks. The contributions of this work are as follows:

●→To resist the potential threat of BWH attacks on blockchain networks, we propose the DF model, which introduces discount factors and withdrawal thresholds to act on rewards.

●→To verify the effectiveness of the proposed model, we conducted theoretical calculations and experimental simulations, which demonstrated that the model can effectively suppress profit-driven BWH attacks.

●→We also analyzed the impact of different withdrawal thresholds in the DF model on attacker rewards and provided a reasonable range of withdrawal thresholds.

The remainder of this paper is structured as follows. Section 2 provides an overview of related work. In Section 3, we present a detailed description of the DF model and its application in modeling BWH attacks. In Section 4, we analyze the impact of BWH attacks in the new model and present the simulation and numerical results. Finally, we conclude this paper in Section 5.

RELATED WORK

Bitcoin basics

Mining process

In the Bitcoin mining process, miners search for random numbers, or *nonces*. They combine the hash value of the previous block, the *Merkle* tree root node containing current transactions, a *nonce*, and a *timestamp* into a data structure and calculate its *sha256* hash. If the resulting value meets the *difficulty* set by the system, a valid block is created. The Bitcoin system automatically adjusts the *difficulty* to maintain an average round duration of 10 minutes. Once a new block is created, it is broadcasted to all nodes in the Bitcoin network. Upon receiving the block, each node writes it into its ledger and continues to derive the next block with this block as the new head. And the miner who generates the new block receives rewards.

Mining pools

Mining pools typically have a manager and several miners. At the beginning of each round, the manager assigns work to the miners, who then calculate the results. The mining pool has its own *difficulty* level, t', which is simpler than the *system-wide difficulty* level, t, in the Bitcoin network. When a miner's computational results satisfy the requirements of t', they have found a block that validates in the pool, called a partial PoW (PPoW) and can submit it to the manager as a share. The manager records the PPoW and distributes rewards at the end of the round based on the number of PPoWs submitted by each miner in the pool. If a miner is fortunate enough to find a block that satisfies the difficulty level t for the entire system, it is called a full PoW (FPoW), and the manager broadcasts it to the Bitcoin network to earn rewards, provided no other competitor exists.

Attack and other resist schemes

Attack model

Attack models for blockchain can be broadly categorized into two types: BWH[10-16] and selfish[17-20]. Other attack models largely stem from improvements to these two types, but this paper focuses on BWH attacks. Rosenfeld[21] first proposed the BWH attack, in which the attacker divides their computational power into two parts: one for honest mining and the other for "penetration" mining in other honest mining pools (target mining pools). However, the latter part does not submit calculated FPoWs to the pool manager but only PPoWs, and shares the pool's profits according to the number of submitted PPoWs. This attack is harmful because the penetration miner impersonates an honest miner and siphons off their share of the pool profits, depriving the target mining pool of the benefits that match its computational power and causing losses. The feasibility of this attack was demonstrated in the 2014 BWH attack against the "Eligius" mining pool, which caused the pool to lose 300 BTC. The attacker used only two accounts and remained undetected for a long time without submitting FPoWs. If the attacker uses multiple accounts, attacks the target mining pool with disguised accounts within a short period, and exits the pool quickly, the attack may go unnoticed. Although the manager can detect the attack by comparing the number of FPoWs and PPoWs submitted by miners during the cycle, there is no effective way to prevent such attacks. BWH attacks can take various forms, such as a single attacker attacking multiple mining pools or multiple attackers attacking a single mining pool, forming a *miners' dilemma*[22] by playing games with each other[23-25].

Other solutions

Numerous papers have proposed solutions to counter BWH attacks. For example, Eyal *et al.*[21,26] proposed the Two-Phase PoW model, while Bag *et al.* proposed the Cryptographic Commitment scheme[27], making it impossible for miners to know whether the computed response is an FPoW required in the network, thus preventing BWH attacks. However, as a reliable model, backward compatibility must be satisfied, and significant changes to the miners' verification logic of the entire model would be impractical for defense purposes. Special Rewards[28] and Incentive Compatible Reward Strategy[29], proposed by Bag *et al.* and Schrijvers *et al.*, respectively, change the incentive mechanism of the block system from the underlying logic, which is innovative but unable to solve practical problems in the current environment. Table 1 shows the underlying logic of these options. Additionally, Luu *et al.*[30] proposed SmartPool, which exists as a mining pool in the system and renders mining pool attacks unprofitable. However, the participants of Bitcoin Forum[31] pointed out that fully adopting this method is still a long and difficult process at present. In contrast, our proposed DF model does not require changes to the current blockchain system from the underlying logic and only changes the reward of each block upon issuance while maintaining the original logic. Such changes are effective for all participants in the system.

DF MODEL AND ASSUMPTION

DF Model

Since block generation can be viewed as a Markov process, we were inspired by the Markov reward process to add a discount factor to the revenue distribution logic of the blockchain system. While the discount factor reduces the revenue obtained by the attacker, the ratio of the attacker's revenue to the total revenue generated by the system remains unchanged, and the attacker can still withdraw the revenue at any time. To limit the attacker's revenue withdrawal, we have added a withdrawal threshold, which prevents miners from withdrawing their rewards from the pool until the threshold is reached. Since the honest miner can join the pool with the same profit expectation as mining alone but can gain faster, this allows the honest miner to join the pool and not leave at will. We have designed a mechanism to weaken the profit of miners who leave the pool by accumulating rounds and applying a discount factor. To preserve the concise structure of the blockchain system, we have not changed the mining process or broadcasting process. Instead, we have added the idea of a discount factor to the reward distribution logic. When the system rewards the mining

Table 1. Resistance logic of existing programs

Scheme Name	Obfuscate the validation logic	Change the incentive mechanism
Two-Phase PoW	√	×
Cryptographic Commitment Scheme	√	×
Special Reward	×	√
Incentive Compatible Reward Strategy	×	√

pool or miner who broadcasts the latest block, it calculates the rewards based on the position of the current broadcasting block in the main chain. The block is marked as n-1, where n is the position of the block on the main chain. The rewards are then multiplied by the marked power of the discount factor, creating an environment in which the attacker focuses on short-term gains. To prevent attackers from extracting rewards immediately after a successful attack to obtain more rewards, we have set a withdrawal threshold. Only when the accumulated rewards of the attacker in the mining pool reach the threshold can they carry out the withdrawal operation and the extracted rewards are based on the number of accumulated rounds in the target mining pool. The rewards received upon withdrawal are the accumulated rewards multiplied by the cumulative number of rounds of the discount factor minus one power. For example, if the attacker experiences ten rounds in the mining pool and reaches the withdrawal threshold, their return is reflected in rewards multiplied by the nine power of the discount factor.

Assumption

To simplify our analysis, we make the same assumptions as most Bitcoin-related papers:

●→Standardizes the Bitcoin system's computational power as 1 so that any computational power is represented as part of the computational power. In addition, it is assumed that no individual miner or pool has a computational power of less than 0.5 to prevent a "51% attack" on the network.

●→No manager or miner launches other attacks except the attacker who launched the BWH attack. We do not consider mixed forms of multiple attacks at the same time in the system, nor do we consider selfish mining attacks and other attacks except BWH attacks.

●→Normalize the rewards to 1 for each valid block instead of the rewards currently given in the actual system.

●→We also consider the existence of natural bifurcation in the model, although the possibility of its occurrence is very small. Based on this assumption, the miner or the pool should get a profit equal to the probability of finding the block in the round; And the probability is going to be equal to the percentage of the computational power in the entire system.

●→When the miners in the mining pool generate FPow, the manager will broadcast the block. When the block becomes a part of the main chain, the manager will get the corresponding rewards. Managers then distribute the rewards to the miners in the pool based on the proportion of shares they submit in the round.

Rewards analysis

We perform mathematical analysis of attackers attacking mining pools under the new model with the following relevant parameters:

α : the computational power of the attacker

β : computational power of target mining pool

τ : the proportion of the attacker's penetration computational power to the attacker's all computational power

c : discount factor value

n : The average number of rounds in which the attacker reaches the withdrawal threshold

The attacker's computational power is α; Among them, β only contains the honest computational power in the honest mining pool, excluding the penetration computational power of the attacker; τ represents the proportion of penetration computational power when an attacker launches an attack; Parameter c is the discount factor value; n represents the number of accumulation rounds in which the average rewards of penetration computation power reaches the withdrawal threshold. Its function is to control the influence of discount factors on earnings. According to the number of accumulation rounds, the discount factors of different powers are assigned to each withdrawal reward. and the n is expressed as Equation1.

$$n = \left\lceil \frac{Withdraw \cdot Threshold}{\mathbb{E}(Reward \cdot of \cdot Penetration)} \right\rceil \tag{1}$$

We divide the behavior of attackers to gain profits into two cases. In the first case, the attacker uses (1-τ)a computational power to get the rewards through honest mining, and in this case, the block generated by FPoW has a successful link reward of (1-τ)a/(1-τa). In the second case, the attacker obtains the proportional rewards from the honest mining pool through penetration computational power. Of course, this kind of reward only exists if the block submitted by the honest mining pool is successfully linked and the rewards are paid to the miners in the mining pool. Since the attacker only accounts for τa/(β+ τa) of the total computational power of the mining pool, the rewards in this case are β/(1- τa)· τa/(β+ τa). Therefore, the reward function of the BWH attack launched in the original model can be expressed as Equation 2.

$$R_\alpha = \frac{(1-\tau)\alpha}{1-\tau\alpha} + \frac{\beta}{1-\tau\alpha} \cdot \frac{\tau\alpha}{\beta+\tau\alpha}, \tag{2}$$

The rewards of attacker R_α are a function of τ. We can find the τ value that maximizes the attacker's rewards in the original model by solving ∂ Ra(τ)/ ∂τ = 0. In the original model, Luu *et al.*[32] proved that when appropriate τ was selected, the return of the BWH attacker would always be greater than the return brought by honest mining. Therefore, in order to obtain the maximum return, the attacker would first allocate penetration computational power and then mine in the target mining pool and by itself. In the new model, due to the existence of a discount factor and withdrawal threshold, the reward function is expressed as Equation 3.

$$R'_\alpha = \frac{(1-\tau)\alpha}{(1-\tau\alpha)\cdot(1-c)} + \frac{n(\frac{\beta}{1-\tau\alpha} \cdot \frac{\tau\alpha}{\beta+\tau\alpha})}{1-c^n} \cdot c^n, \tag{3}$$

Since there is no solution for solving ∂ R'a(τ)/ ∂τ=0, it can be seen that τ, which maximizes the return, exists at the endpoints; that is, τ = 0 or τ = 1, which, respectively, means no BWH attack or use all computational power to carry out BWH attack. Since the partial derivative is less than 0, the original function is monotonically decreasing, that is, τ = 0 will get the maximum benefit, that is, no attack will be launched in the new model, and honest mining will get the highest benefit.

RESULT ANALYSIS

In this section, we analyze the effect of the BWH attack in the new model from three perspectives to demonstrate our theory. Firstly, we analyze the effect of attackers attacking the target mining pool at different rates of penetration in the new model. Secondly, we compare the effect of honest mining with its own computational power and launching attacks with a certain rate of penetration from the perspective of rewards in the new model. Thirdly, we compare the effect of the BWH attack launched by the attacker in the new model with the original model to prove our theory. Additionally, we analyze the influence of the withdrawal threshold on rewards and provide a reasonable range for the withdrawal threshold. In the experiments, we set the discount factor to 0.8 after several trials and set the withdrawal threshold to the median value within the range. To obtain our results, we calculated the theoretical data using Matlab and then simulated the experimental environment to obtain the experimental data. For the simulation experiments in this paper, a blockchain network simulation environment was implemented in IntelliJ IDEA via Java language(JDK 1.7) on a computer with Win 10 system loaded with 4GB RAM and i7 CPU, where a total of 1000 miners were set up and assigned to different mining pools according to the experimental requirements to form mining pools with different computing power. Each experimental data in the experiment generates 1 million blocks and analyses the reward for every thousand blocks, where the average computation time for each data is 32 minutes.

The effect of different rates of penetration

In this section, we investigate whether there is a benefit interval for attackers to launch BWH attacks in the new model. We set the attacker's and the target mining pool's computational power to fixed values and examine whether there is a benefit interval for the attacker by observing the changing trend of the attacker's rewards in the new model as the attacker's rate of penetration to the target mining pool changes. Specifically, we set the computational power of both the attacker *(α)* and the target mining pool *(β)* to 0.2, the discount factor *(c)* to 0.8, the withdrawal threshold to 0.5, the rate of penetration *(τ)* to∈[0.05, 1], and the growth step to 0.05.

Figure 1 shows that, based on the calculated theoretical results, the attacker's rewards in the new model exhibit a downward trend with the continuous increase of the attacker's penetration rate. Moreover, there is no benefit interval within the range of penetration rates for this computational power combination. The experimental results are consistent with our theoretical curve. This indicates that the attacker does not gain any benefits from launching attacks in the new model, and the more computational power the attacker applies to the target mining pool, the greater the loss incurred by the attacker.

Compare the rewards of honest mining and launching a BWH attack in the new model

To compare the impact of launching attacks with honest mining on rewards under the new model with the same computational power and confirm whether the attacker has a benefit point within the range of controllable computational power, we set the computational power of the target mining pool *(β)* to 0.2, the penetration rate *(τ)* to 0.2, the discount factor *(c)* and the withdrawal threshold to 0.8 and 0.5, respectively. We vary the computational power of the attacker *(α)* within the range of [0.06, 0.5], with a growth step of 0.02.

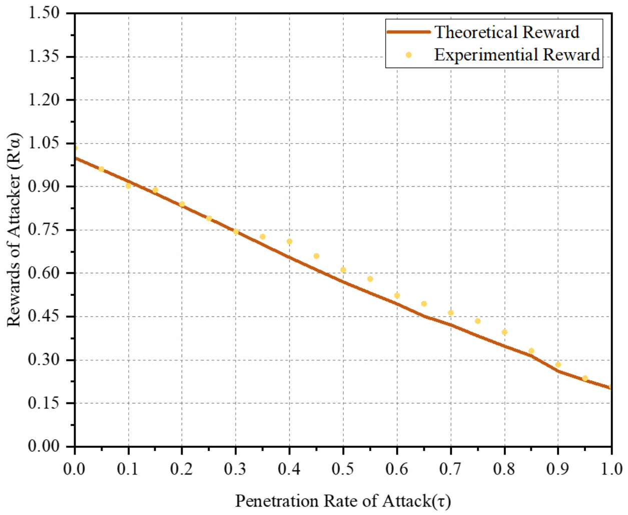

Figure 1. The changing trend of rewards of attackers with different penetration rates.

The theoretical results shown in Figure 2 indicate that the rewards of honest mining and attacking by the attacker using its computational power increase with the computational power, which is consistent with the original model where the higher the proportion of computational power in the whole system, the higher the rewards. Additionally, we observe that under the new model, the rewards of honest mining are consistently higher than the rewards of launching an attack, and as the computational power increases, the gap between the rewards of launching an attack and the rewards of honest mining widens. Our simulation results also align with our theoretical rewards. Therefore, it is evident that the attacker incurs negative rewards from launching attacks in the new model.

Compare the rewards of the original model and the new model at same attack computational power

To verify the attack performance of the same attacker in the original model and the new model and confirm the inhibitory effect of the new model on BWH attacks, we select the attacker to launch attacks in both the original and new models with the optimal penetration computational power in the original model. We measure the proportion of rewards obtained by the attacker in the current cycle (1000 blocks) as the standard of measurement and use the variation trend of the rewards ratio to demonstrate the difference in launching attacks between the two models. We set the computational power of the attacker to 0.2 *(α)*, and the discount factor *(c)* and withdrawal thresholds in the new model to 0.8 and 0.5, respectively. The computational power of the target mining pool *(β)* ranges from 0.06 to 0.5, with a growth step of 0.02. The penetration rate varies with the computational power of the target mining pool.

The proportion of rewards of the attacker to the total rewards of the whole system in 1000 rounds is represented by $R_p = R_a/R_{all}$ where R_α is the rewards of the attacker, and R_{all} is the total rewards of the whole system in 1000 rounds. As shown in Figure 3, in the new model, when the attacker uses the optimal computational power to launch attacks on the target mining pool, the attacker's rewards exhibit a continuous decline trend, even as the computational power of the target mining pool increases. In contrast, in the original model, under the condition of using the optimal penetration computational power, the attacker's rewards increase with the increase of the target mining pool's computational power. Our simulation results are consistent with the theoretical data, indicating that the new model suppresses attackers in terms of rewards compared to the original model, thereby deterring attackers from launching attacks on the target mining pool for the purpose of rewards.

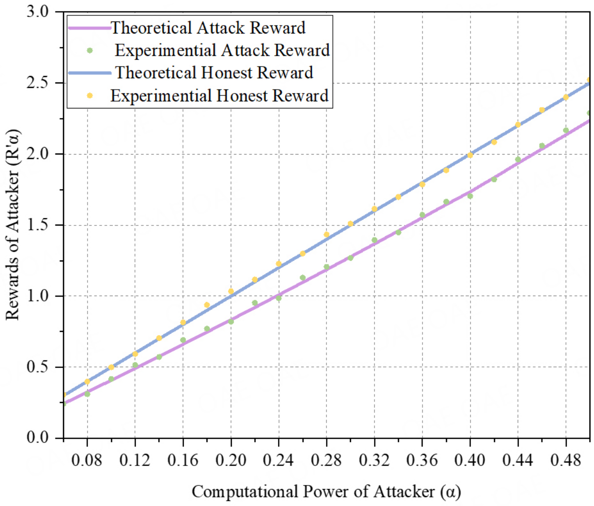

Figure 2. The rewards of launching an attack and honest mining under the same computational power.

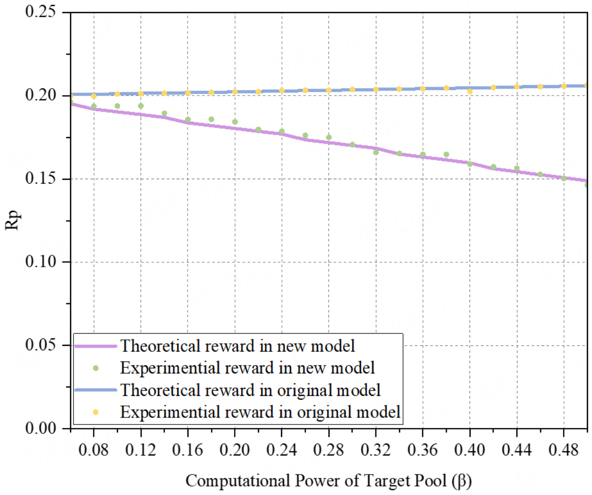

Figure 3. The rewards of launching the same attack in the new model and the original model.

The impact of different withdrawal thresholds

In this section, we aim to effectively demonstrate the impact of the withdrawal threshold on earnings by considering an extreme scenario where the attacker uses all of its computational power as penetration computational power to launch attacks on the target mining pool. To observe the influence of different withdrawal thresholds on the attacker's earnings in this scenario, we set the computational power of both the attacker (α) and the target mining pool (β) to 0.2. The discount factor (c) is 0.8, the penetration rate (τ) is set to 1, and the withdrawal threshold is varied within the range of [0.1, 1], with a growth step of 0.1.

The theoretical results shown in Figure 4 demonstrate a downward trend in the attacker's rewards with an increase in the withdrawal threshold, and our simulation results are consistent with this theory. This indicates that the withdrawal threshold setting in the new model forces the attacker to wait for a long time before obtaining benefits, thereby allowing the discount factor to act on the benefits of the attacker and effectively weakening the rewards gained by launching BWH attacks. Although this experiment considers an extreme case, attackers typically use only a portion of their computational power as penetration

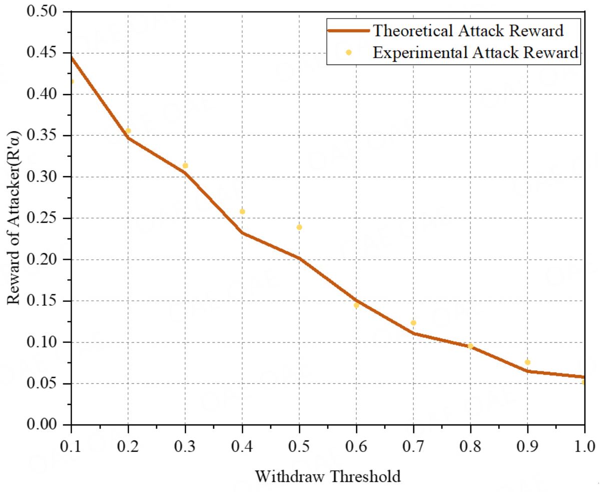

Figure 4. The impact of different withdrawal thresholds on attacker's rewards.

computational power to launch attacks in order to gain benefits. However, in the new model, the rewards obtained by such low computing power are negligible, and it is difficult to reach the withdrawal threshold. To effectively limit attackers from launching attacks, we recommend setting the withdrawal threshold at 0.3 or above.

CONCLUSION

Given the potential threat of BWH attacks to blockchain networks, this paper proposes a novel blockchain model that incorporates two parameters, a discount factor and a withdrawal threshold, to weaken the gains obtained by attackers in the target mining pool and make withdrawals difficult. Our approach ensures that the gains of miners in the mining pools remain stable while causing the gains obtained by attackers launching attacks to exhibit negative growth. We validate the effectiveness of our model through theoretical arguments and simulation experiments, demonstrating that it can effectively suppress profit-oriented BWH attacks.

DECLARATIONS

Authors' contributions

Made substantial contributions to the conception and design of the study and performed data analysis and interpretation: Xiao Z, Zhang F

Performed data acquisition and provided administrative, technical, and material support: Wei B

Availability of data and materials

Not applicable.

Financial support and sponsorship

The Innovation Project of GUET Graduate Education under project 2022YCXS073.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Available from:https://assets.pubpub.org/d8wct41f/31611263538139.pdf [Last accessed on 6 May 2023].
2. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Available from: https://mnmarketcap.com/wp-content/uploads/2022/09/Ethereum-Whitepaper.pdf [Last accessed on 6 May 2023].
3. Yutaka M, Zhang Y, Sasabe M, et al. Using ethereum blockchain for distributed attribute-based access control in the internet of things. 2019 IEEE Global Communications Conference (GLOBECOM); 2019 Dec 1-6. DOI
4. Wang W, Chen Q, Yin Z, et al. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet Things J* 2022;9:8883-91. DOI
5. Lian Z, Zeng Q, Wang W, Gadekallu TR, Su C. Blockchain-based two-stage federated learning with non-IID data in IoMT system. *IEEE Trans Comput Soc Syst*. DOI
6. Gadekallu T R, Huynh-The T, Wang W, et al. Blockchain for the metaverse: a review. arXiv preprint arXiv:2203.09738, 2022. DOI
7. Gjermundrød H, Chalkias K, Dionysiou I. Going beyond the coinbase transaction fee: alternative reward schemes for miners in blockchain systems. Proceedings of the 20th Pan-Hellenic Conference on Informatics. 2016 Nov 1-4. DOI
8. Recabarren R, Carbunar B. Hardening stratum, the Bitcoin pool mining protocol. *Proceedings on Privacy Enhancing Technologies* 2017;2017:57-74. DOI
9. Fujita K, Zhang Y, Sasabe M, Kasahara S. Mining pool selection under block withHolding attack. *Applied Sciences* 2021;11:1617. DOI
10. Courtois N T, Bahack L. On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718, 2014. DOI
11. Dong X, Wu F, Faree A, Guo D, Shen Y, Ma J. Selfholding: a combined attack model using selfish mining with block withholding attack. *Computers & Security* 2019;87:101584. DOI
12. Chang S, Park Y, Wuthier S, Chen C. Uncle-block attack: blockchain mining threat beyond block withholding for rational and uncooperative miners. In: Deng RH, Gauthier-umaña V, Ochoa M, Yung M, editors. Applied Cryptography and Network Security. Cham: Springer International Publishing; 2019. pp. 241-58. DOI
13. Qin R, Yuan Y, Wang F. Optimal block withholding strategies for blockchain mining pools. *IEEE Trans Comput Soc Syst* 2020;7:709-17. DOI
14. Kwon Y, Kim D, Son Y, et al. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017 Oct 195-209. DOI
15. Yang R, Chang X, Misic J, Misic V, Kang H. On selfholding attack impact on imperfect PoW blockchain networks. *IEEE Trans Netw Sci Eng* 2021;8:3073-86. DOI
16. Gao S, Li Z, Peng Z, et al. Power adjusting and bribery racing: Novel mining attacks in the bitcoin system. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security; 2019 Nov 833-850. DOI
17. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. *Commu ACM* 2018;61:95-102. DOI
18. Nayak K, Kumar S, Miller A, et al. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. 2016 IEEE European Symposium on Security and Privacy; 2016 Mar 305-320. DOI
19. Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin. In: Grossklags J, Preneel B, editors. Financial Cryptography and Data Security. Berlin: Springer Berlin Heidelberg; 2017. pp. 515-32. DOI
20. Li T, Wang Z, Yang G, Cui Y, Chen Y, Yu X. Semi-selfish mining based on hidden Markov decision process. *Int J Intell Syst* 2021;36:3596-612. DOI
21. Rosenfeld M. Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980, 2011. DOI
22. Eyal I. The miner's dilemma. 2015 IEEE Symposium on Security and Privacy; 2015 89-103. DOI
23. Toda K, Kuze N, Ushio T. Mining pool game model and nash equilibrium analysis for PoW-based blockchain networks. DOI
24. Li W, Cao M, Wang Y, Tang C, Lin F. Mining pool game model and nash equilibrium analysis for PoW-based blockchain networks. *IEEE Access* 2020;8:101049-60. DOI
25. Haghighat A A, Shajari M. Block withholding game among bitcoin mining pools. *Future Generation Computer Systems* 2019;97:482-91. DOI
26. Eyal I, Sirer E G. How to disincentivize large bitcoin mining pools. Available from: https://hackingdistributed.com/2014/06/18/how-to-

disincentivize-large-bitcoin-mining-pools/ [Last accessed on 6 May 2023].

27. Bag S, Ruj S, Sakurai K. Bitcoin Block Withholding Attack: Analysis and Mitigation. *IEEE Trans Inform Forensic Secur* 2017;12:1967-78. DOI

28. Bag S, Sakurai K. Yet another note on block withholding attack on bitcoin mining pools. In: Bishop M, Nascimento ACA, editors. Information security. Cham: Springer International Publishing; 2016. pp. 167-80. DOI

29. Schrijvers O, Bonneau J, Boneh D, Roughgarden T. Incentive compatibility of bitcoin mining pool reward functions. In: Grossklags J, Preneel B, editors. Financial cryptography and data security. Berlin: Springer Berlin Heidelberg; 2017. pp. 477-98. DOI

30. Luu L, Velner Y, Teutsch J, et al. SMART POOL: practical decentralized pooled mining. Available from: https://ia.cr/2017/019 [Last accessed on 6 May 2023].

31. Available from: https://bitcointalk.org/index.php?topic=18313.14900 [Last accessed on 6 May 2023].

32. Luu L, Saha R, Parameshwaran I, et al. On power splitting games in distributed computation: the case of bitcoin pooled mining. 2015 IEEE 28th Computer Security Foundations Symposium; 2015 397-411. DOI