

Mitigating Double-Spending and Selfish Mining Attacks in Blockchain Networks

Zimeng Gu^a

School of Computer Science, Xi'an Jiaotong University City College, Xi'an, China


Keywords: Double-Spending Attack; Selfish Mining; Blockchain Security; Defense Mechanisms.

Abstract: Blockchain technology offers significant potential across various fields due to its decentralized and tamper-proof nature. However, it is not without its security challenges. This paper focuses on two prominent attacks in blockchain networks: double-spending and selfish mining. It provides a detailed explanation of the double-spending attack, highlighting how it exploits confirmation time differences and transaction revocability to enable the repeated spending of the same digital asset. This attack can result in substantial damage to user assets and undermine system trust. In contrast, selfish mining involves a miner-controlled node deliberately withholding mined blocks to increase its chances of block confirmation. This behavior can disrupt the consensus mechanism, impair system efficiency, and compromise fairness. The paper also explores existing defense mechanisms against these attacks, including enhancements to transaction confirmation processes, the application of advanced cryptographic techniques, and the strengthening of regulatory measures. Additionally, it examines the optimization of consensus algorithms, adjustments to incentive mechanisms, and the establishment of effective monitoring and warning systems. The aim is to provide insights that can enhance blockchain security and support the stable development of blockchain technology.

1 INTRODUCTION

Blockchain, as a decentralized distributed database technology, originated from Satoshi Nakamoto in 2008, and its core concept is to ensure the tamperability and security of data through encryption algorithms and distributed ledger technology (Zheng et.al, 2017). Blockchain technology is characterized by its unique "unforgeable", "full traceability", "traceability", "openness and transparency" and "collective transparency". Because of its unique characteristics of "non-falsification", "full traceability", "traceability", "openness and transparency" and "collective maintenance", blockchain technology has been widely used in finance, government affairs, supply chain management, intellectual property rights and other fields, which greatly improves the transaction efficiency and data security. However, with the popularization and in-depth application of blockchain technology, its security, privacy protection and performance issues have gradually become research topics that cannot be ignored (Cao et.al, 2021).

In a blockchain network, there may be many different ways to attack the same security vulnerability or attack target. According to the blockchain level of the attack vulnerability or target, the existing blockchain attack methods can be classified as follows (Tian et.al, 2021; Bhargavan et.al, 2016): First, data layer attacks include data privacy theft: attackers steal sensitive data on the blockchain through various means, such as transaction information and user identity. Malicious data attack: The injection of false or malicious data into the blockchain to compromise the integrity and trust of the data; Second, network layer attacks include node attacks: disrupting the normal operation of the blockchain by controlling or hijacking network nodes. Peer to Peer network attacks: Use the peer-to-peer (P2P) network characteristics of blockchain to implement a variety of network attacks, including Distributed Denial of Service attacks (Saad et.al, 2018); Third, consensus layer attacks include 51% attacks (Aponte-Novoa et.al, 2021): by controlling more than 50% of the network computing power, the attacker implements malicious behaviors such as

^a <https://orcid.org/0009-0008-3454-8409>

double payment and rewriting the blockchain history. Malicious chip acquisition: Obtaining mining chips through improper means, affecting the consensus process of the blockchain; Fourth, contract layer attacks include smart contract vulnerability attacks (Liu and Ruan, 2021): exploit vulnerabilities in smart contracts to execute malicious code, resulting in asset loss or system crash. Contract virtual machine attacks: attacks against the smart contract execution environment, affecting the correct execution of contracts; Fifth, application-layer attacks include mining scenario attacks: attacks against the mining system and mining mechanism, affecting the mining efficiency and security of the blockchain. Trading scenario attacks: trading platform attacks, user account attacks, etc., directly threaten the security of user assets.

To address the various attacks on blockchain systems, existing literature suggests several defense mechanisms. Enhancing consensus mechanisms is crucial; distributed consensus protocols, such as proof-of-work (PoW) and proof-of-stake (PoS), help ensure that all nodes in the network reach agreement and prevent any single node or small group of nodes from maliciously manipulating the system. Additionally, strengthening the security design of network protocols and applications is important. Implementing traffic cleaning and filtering mechanisms can reduce the risk of network attacks, including Denial of Service (DoS) attacks, thereby improving overall network resilience. Furthermore, conducting regular security audits of smart contracts is essential. These audits help identify and address vulnerabilities promptly, establish security standards and best practices, and offer reporting and reward mechanisms to incentivize the discovery of contract vulnerabilities. Together, these strategies form a comprehensive approach to enhancing blockchain security and mitigating potential threats.

2 METHODOLOGIES

The primary objective of this study is to provide a comprehensive analysis of blockchain attacks, including their mechanisms, types, and defense strategies. The paper is organized into five main sections, as illustrated in Figure 1. Firstly, it presents an overview of the fundamental concepts and background related to blockchain attacks. This section clarifies the basic principles and characteristics of blockchain technology, along with the definitions, classifications, and risks associated with blockchain attacks, establishing a foundation for

the subsequent analysis. Secondly, the study delves into the core techniques of blockchain attacks, focusing on the technical principles and implementation processes of prominent methods such as Double Spending Attacks and Selfish Mining Attacks. This analysis reveals the security vulnerabilities and underlying attack logic of these methods.

Thirdly, the paper demonstrates and evaluates the performance of key blockchain attack techniques through case studies and empirical data. It assesses the specific effects and degree of harm caused by these attacks, providing insight into their impact on system security. Fourthly, the discussion turns to the advantages and limitations of current blockchain security technologies, examining existing research results and technological trends. This section explores the strengths and weaknesses of these technologies and anticipates future development directions and emerging research hotspots. Finally, the paper concludes with a summary of the research content and main findings, highlighting current research gaps and suggesting future research directions. This summary aims to provide valuable references for ongoing and future studies in the field of blockchain security.



Figure 1: The pipeline of the study (Picture credit: Original).

2.1 Double Spending

A double spender is an attacker who attempts to make multiple payments with the same asset on a blockchain network. The attacker uses the ability to control a large amount of arithmetic power to "undo" the originally confirmed transaction in the network and eventually return the transaction to their wallet by creating a replacement block. This attack is common on blockchains with proof-of-work mechanisms. Cryptocurrencies and blockchain had been under development for many years before Bitcoin was introduced. One of the many reasons they didn't work until Bitcoin was that an issue needed to be resolved—one where a user could alter the information on a distributed ledger to give themselves back any tokens they had spent.

This is a weakness in any digital money system, which is why third-party auditors have traditionally been involved. These auditors must spend time,

which equates to money, verifying transactions and amounts between parties. For this system to work, there must be trust between all parties involved that the auditors, ledger maintainers, or other parties would not alter entries to benefit themselves or others. The structure of the double spending is shown in the Figure 2.

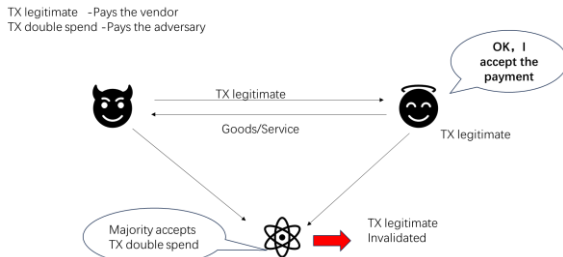


Figure 2: The process of double spending (Picture credit: Original).

The most significant double-spending risk for blockchains is a 51% attack (Aponte-Novoa et.al, 2021), which can occur if an entity controls more than 50% of the hashing power or validation mechanisms on a network. If this user—or users—assumes a majority of the network, the network's stake, or any other mechanism used, they will be able to dictate transaction consensus and control the award of currency. New or forked cryptocurrencies with smaller networks are susceptible to this attack. In cryptocurrency networks such as Bitcoin, this is very unlikely due to the number of network participants and the speed at which the network operates.

Ethereum uses a staking mechanic, where only those users who have locked large amounts of ether in smart contracts can become validators and propose blocks. To attempt this attack, a group or entity would need to control more than 50% of the staked ether on the network—a very costly effort because 32 Ethereum (about \$95,200 at the May 15, 2024 price) is required to establish a node, and there is also a mechanism that burns the tokens of dishonest validators.

There are three common types of attacks in double spending: To begin with, the Race Attack, also called unconfirmed transaction, are where a malicious user attempts to send two quick transactions, one to a recipient and one to the blockchain. The one to a recipient might transfer a token to them, but the transaction sent to the network would keep it in the sender's possession. This is an attempt to exploit network lag, with the sender's transaction establishing ownership being confirmed first. This is easily prevented by not accepting unconfirmed transactions. Apart from that, the Finney Attack (Liu and Ruan,

2021), named after Hal Finney, the developer who pointed out the weakness, is a type of unconfirmed transaction attack. However, this attack requires a miner, who creates a block and sends an amount to two addresses they own. Another transaction is sent to another party in the same block. If the recipient accepts it before it is confirmed by the network, the sender can essentially return the amount sent and spend it again. This attack is very rare on large blockchains but can be prevented by not accepting unconfirmed transactions or using a wallet that doesn't let researchers accept them.

The last one is Sybil Attack (Liu and Ruan, 2021), it is a technique in which attackers create a large number of fake identities to increase their influence over the network and manipulate it. Attackers can use these fake identities to exert control. Attackers can use these fake identities to exert control over the consensus process, potentially disrupting the network and causing denial-of-service conditions.

2.2 Selfish Mining

Selfish Mining is a strategy in which miners do not publicize the blocks they mine, but instead try to keep these blocks private in order to increase their own earnings (Liu and Ruan, 2021). If these miners are able to successfully publish their blocks in the public blockchain, they are able to allow other miners to waste arithmetic while they themselves are rewarded more. This approach can effectively weaken other miners' arithmetic power while increasing the profits of selfish miners.

As for its working operation, "Mining" is the process via which nodes in a blockchain network verify and validate transactions. Tokens that have just been created are awarded to miners for their computational efforts. A cartel hides newly formed blocks from the main chain and reveals them later as part of a self-serving mining plan.

Researchers Emin Gün Sirer and Ittay Eyal from Cornell University first recognized selfish mining in a 2013 publication. They showed that it is possible to create a blockchain branch and earn extra bitcoins by keeping newly generated blocks concealed from the main chain. In theory, miners have the ability to add it to the network at right moment and change the blockchain (Eyal and Sirer, 2018).

The proof-of-work consensus mechanism used by Bitcoin and other cryptocurrency networks depends on miners whose software solves cryptographic puzzles. A new block appears on the blockchain when the hash is deciphered, and the miner or miners who

solved it are rewarded and receive a transaction fee (Nakamoto, 2008).

By hiding new blocks and making them available to systems only within their private network (Eyal and Sirer, 2018), miners can increase their overall income share, as demonstrated by Sirer and Eyal in their 2013 study. This procedure speeds up the process of discovery and fixes mining-related infrastructure problems including network latency and electricity expenses.

The split blockchain would start off shorter than the main chain. Within its pool, the private chain mines new blocks, hiding any that are created outside of it. Until the private blockchain reaches a block height higher than the public blockchain, the mining process is repeated.

Then, self-serving miners carefully plan when to add their new blocks to the honest blockchain, allowing the public blockchain to merge with the just added chain. The new blockchain is mined by the public network, and the transaction fees and cryptocurrency incentives go to the egotistical miners for their freshly approved blocks.

Sirer and Eyal looked over the resources that both chains had wasted. They postulated that since their rewards were comparatively larger when accounting for resource consumption, selfish miners had an advantage over other miners on the public blockchain (Eyal and Sirer, 2018).

It's also widely discussed that selfish mining attacks pose a threat. Sirer and Eyal gave convincing proof of how to modify a blockchain by causing a split and outpacing truthful miners. They also said that logical miners will join the organization because they are lured to the higher payouts (Eyal and Sirer, 2018) and will notice the group's profits. On the other hand, some scholars disagree about the motivations, viability, and dangers presented by self-centered miners and organizations.

In 2017, Craig Wright proved that if miners were honest (Wright and Savanah, 2017), they would not create more blocks and so receive more rewards than they were previously entitled to. Jake Guber postulated in 2018 that many miners might engage in selfish mining if it were more profitable than honest mining. Jake demonstrated how, even if selfish mining is more profitable than honest mining, a network's profitability would be negatively impacted by numerous selfish miners or groups causing a race between the forks (Guber, 2018). It's interesting to note that, according to Zhaojie Wang and colleagues' research, there had not been any documented instances of selfish mining attacks in the actual world as of the end of 2021 (Wang et.al, 2021).

While selfish mining assaults may happen, the arguments on both sides imply that they might only be academic in nature. Another possibility is that there has already been a self-serving mining attack that has gone unreported. On the other hand, the majority of 1bitcoin miners most certainly have good intentions, and more widely used blockchains are safe due to the large number of users. A blockchain gets more secure and processes information more quickly the more network users it has. Even with a wellorganized group of attackers, the Bitcoin network is just too big and too quick to take over.

2.3 Preventive Mechanism

At present, there are many preventive mechanisms. This paper discusses the following defense mechanisms. For double-spending attack, first of all, increasing the transaction confirmation time can reduce the chance of a double-spending attack occurring within a shorter time frame. Additionally, using multi-signature technology requires multiple parties to sign off on a transaction, making it more difficult for an attacker to execute a double-spend.

Second, digital signature technology ensures the authenticity and integrity of transactions, preventing them from being tampered with. Hash function technology converts transaction information into a unique hash value that serves as a distinct identifier, making it hard for the same asset to be spent twice. Third, Enhanced supervision of digital currency trading platforms can implement security measures like multi-signature and digital signature technologies to increase transaction security. Regulating digital currency mining can also prevent double-spending attacks by ensuring miners use legal equipment and follow proper mining rules.

For selfish-mining attack, firstly, improving the proof-of-work algorithm or adopting new consensus algorithms such as proof-of-stake or delegated proof-of-stake can increase the security and efficiency of the blockchain and reduce the likelihood of selfish mining. Hybrid consensus algorithms that combine different algorithms can also be explored. Secondly, Modifying the mining reward mechanism to distribute rewards based on miner contributions can reduce the incentive for selfish mining. Introducing penalty mechanisms for selfish miners, such as fines or reduced credibility, can increase the cost of engaging in selfish mining.

Thirdly, establishing monitoring and early warning systems, a monitoring system can detect abnormal transactions and mining behaviors in real time. An early warning system can send alerts

promptly when anomalies are detected, enabling users and regulators to take timely action.

3 RESULT AND DISCUSSION

The effectiveness of the defense mechanisms against double-spending attacks and selfish mining is a crucial topic. On one hand, transaction confirmation mechanisms, such as increasing confirmation time and using multi-signature technology, can reduce the likelihood of double-spending. However, longer confirmation times may lead to slower transactions and inconvenience for users. Digital signature and hash function technologies enhance security but add computational complexity. Regulatory measures are important but may face challenges in implementation and enforcement.

For selfish mining, optimizing consensus algorithms can improve system security and efficiency. But it requires extensive research and experimentation. Adjusting incentive mechanisms can discourage selfish behavior, but finding the right balance to maintain miner motivation is difficult. Monitoring and early warning systems are valuable but need continuous improvement to keep up with evolving attack methods. Moreover, the interaction between different defense mechanisms needs to be considered. A comprehensive approach that combines multiple measures may be more effective than relying on a single method. However, this also increases the complexity and cost of the system. As blockchain technology continues to evolve, so must the defense mechanisms to stay ahead of potential attacks.

4 CONCLUSIONS

This paper provides an in-depth analysis of double-spending and selfish mining attacks within blockchain networks. It focuses on examining the principles, impacts, and defense strategies associated with these two types of attacks. For double-spending attacks, the paper emphasizes several defensive measures, including enhancing transaction confirmation mechanisms, implementing advanced encryption technologies, and strengthening regulatory oversight. In addressing selfish mining, the study highlights the importance of optimizing consensus algorithms, adjusting incentive structures, and establishing robust monitoring and early warning systems. The findings reveal that while these

defensive strategies offer distinct advantages, they also have limitations. Moving forward, it is essential to continuously monitor advancements in blockchain technology and explore new attack vectors. Ongoing research and optimization of defense mechanisms will be crucial to maintaining the security and stability of blockchain systems.

REFERENCES

- Aponte-Novoa, F.A., Orozco, A.L.S., Villanueva-Polanco, R., & Wightman, P., 2021. The 51% attack on blockchains: A mining behavior study. *IEEE access*, 9, 140549-140564.
- Bhargavan, K., Delignat-Lavaud, A., Fournet, C., et al. 2016. Formal verification of smart contracts: Short paper. *Proceedings of the ACM workshop on programming languages and analysis for security*, 91-96.
- Cao, X.L., Zhang, J.H., Liu, B., 2021. A review of blockchain security, privacy and performance issues. *Computer integrated manufacturing system*, 27(7), 2078-2094.
- Eyal, I., Sirer, E.G., 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7), 95-102.
- Gober, J.A., 2018. The Dynamics of a "Selfish Mining" Infested Bitcoin Network: How the Presence of Adversaries Can Alter the Profitability Framework of Bitcoin Mining.
- Liu, H.Q., Ruan, N., 2021. Research on attack modes in blockchain. *Journal of Computer science*, 44(4), 786-805.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.
- Saad, M., Thai, M.T., Mohaisen, A., 2018. POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization. *Proceedings of the Asia conference on computer and communications security*, 809-811.
- Tian, G.H., Hu, Y.H., Chen, X.F., 2021. Research progress on attack and defense techniques in block-chain system. *Journal of Software*, 32(5), 1495-1525.
- Wang, Z., Lv, Q., Lu, Z., et al. 2021. ForkDec: accurate detection for selfish mining attacks. *Security and Communication Networks*, 2021(1), 5959698.
- Wright, D.C.S., Savanah, S., 2017. The fallacy of the selfish miner in bitcoin: An economic critique. Available at SSRN 3009466.
- Zheng, Z., Xie, S., Dai, H., et al. 2017. An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE international congress on big data*, 557-564.