Analyzing Vulnerabilities of Bitcoin: A Study of Sybil, Finney, and Vector76 Attacks and Their Mitigation Strategies

Qinhan Ren[a]
School of Cyber Engineering, Xidian University, Xi'an, China

Keywords: Bitcoin, Sybil Attack, Finney Attack, Blockchain Networks.

Abstract: This study explores three critical attack vectors includes Sybil, Finney, and Vector76 that pose significant threats to the security of Bitcoin and other blockchain networks. The research analyzes the mechanics of each attack and evaluates their success rates under different network conditions. The Sybil attack is examined in the context of node creation and identity manipulation in decentralized networks. The Finney attack is analyzed for its exploitation of transaction timing vulnerabilities, while the Vector76 attack is studied for how it leverages network propagation delays to achieve double spending. By investigating these attack mechanisms, the study identifies network synchronization and enhanced transaction processing as potential mitigation strategies. The findings highlight the importance of improving block propagation speeds and real-time monitoring systems to strengthen the resilience of blockchain networks. These insights offer valuable guidance for developers and researchers working to bolster the security and stability of decentralized systems, ensuring better protection against evolving threats in cryptocurrency environments.

1 INTRODUCTION

The growth of blockchain techniques and cryptocurrencies promote the Bitcoin to become the bedrock in the digital economy. Bitcoin, which is a decentralized cryptocurrency, operates on a peer-to-peer network without a central authority. Meanwhile it ensures the transparency and security by cryptographic techniques and the Proof of Work (PoW) consensus mechanism (Nakamoto, 2008). This decentralized nature contains several vulnerabilities, which makes the network susceptible when it faces to various forms of attack. Among these critical threats are the Sybil, Finney, and Vector76 attacks. They not only exploit different parts of Bitcoin's infrastructure but also target their consensus mechanism, transaction verification, and propagation processes (Bonneau et.al, 2015). Understanding and mitigating these attacks is significant for the security and stability of Bitcoin and other cryptocurrencies which has been built on the similar consensus mechanism. These attacks not only threaten the integrity of transactions but also undermine the trust in the overall network system.

First introduced by Douceur in 2002, the Sybil attack is one of the most considered forms of attack in the decentralized systems (Douceur, 2002). In this attack, a single malicious actor creates multiple identities in a network to obtain disproportionate control over the system, which potentially disrupts consensus. Although The Sybil attack is always problematic in peer-to-peer networks, Bitcoin's PoW mechanism provides some protection like making identity creation costly through mining. Nevertheless, this cannot completely prevent such attack, since powerful adversaries companied by significant computational resources could still influence the network (Heilman et.al, 2015). On the other hand, the Finney attack, which has been first described by Bitcoin creator Satoshi Nakamoto, exploits the concept of double-spending by pre-mining a block which contains a transaction and broadcasting it after transaction has been accepted (Karame et.al, 2012).While this attack might be rare, it highlights a fundamental vulnerability in the method which used by the Bitcoin when it handles transaction finality and trust. The Vector76 attack is an advanced form of double-spending. It combines elements of the Finney attack with race attacks. In that case, the Vector76

[a] https://orcid.org/0009-0002-6613-8902

Ren and Q.
Analyzing Vulnerabilities of Bitcoin: A Study of Sybil, Finney, and Vector76 Attacks and Their Mitigation Strategies.
DOI: 10.5220/0013525400004619
In *Proceedings of the 2nd International Conference on Data Analysis and Machine Learning (DAML 2024)*, pages 428-431
ISBN: 978-989-758-754-2

attack could take advantage of the timing between transaction confirmation and block propagation to defraud recipients (Decker and Wattenhofer, 2014).

Nowadays, growing researches have been handled to mitigate these vulnerabilities. Bonneau et al. provided a comprehensive overview of the challenges of Bitcoin, which contains vulnerabilities of Bitcoin like the Sybil Attack (Bonneau and et.al, 2015). Their work emphasized the importance of network design and consensus mechanisms in protecting the cryptocurrency under these threats. Moreover, Heilman et al. raised the concept of eclipse attacks. It is a variant of Sybil attacks which isolates nodes from the rest of the network. Hence, it allows adversaries to control the victim's view of the blockchain. Solutions of that attack such as increasing the number of block confirmations, implementing stronger identity verification systems, or even boosting node communication protocols have been introduced to face to these attacks Bitcoin continues to evolve (Rosenfeld, 2014). However, the methods used by attackers keep to update (Wen et.al., 2021). It necessitates ongoing research and updates of the Bitcoin protocol (Hamdi et. al., 2024).

This paper aims to provide a thorough review of the various attacks that present significant threats to blockchain systems, with a particular focus on how these attacks compromise the integrity, security, and functionality of blockchain networks. As decentralized platforms, blockchains are vulnerable to a wide range of attack vectors, such as 51% attacks, double-spending attacks, Sybil attacks, and smart contract vulnerabilities. These threats can undermine the trust and reliability of blockchain systems, posing severe consequences for applications such as cryptocurrency transactions, decentralized finance (DeFi), and other sectors relying on blockchain technology (Gervais et al., 2016).

The paper not only categorizes these attacks based on their methodology and potential damage but also critically evaluates the existing defense strategies employed by blockchain networks. These defense mechanisms include consensus algorithms (like Proof of Work and Proof of Stake), cryptographic techniques, network monitoring, and smart contract auditing tools. While some strategies have proven effective in mitigating certain threats, this paper highlights their limitations in addressing more sophisticated or evolving attack methods. For instance, while Proof of Work offers strong security through decentralization, it is energy-intensive and may lead to mining centralization, which itself presents security risks.

Furthermore, this study explores future directions for bolstering blockchain security. It delves into emerging defense strategies such as hybrid consensus mechanisms, zero-knowledge proofs, and machine learning-based anomaly detection. By analyzing these approaches, the paper seeks to offer insights into potential innovations that could enhance blockchain resilience. Ultimately, the analysis contributes to a deeper understanding of the evolving challenges in blockchain security, aiming to guide future research and development efforts in creating more secure and robust blockchain ecosystems.

2 METHODOLOGIES

2.1 Research Process

The primary objective of this study is to analyze the vulnerabilities in consensus mechanism of Bitcoin by focusing on three specific attack vectors: Sybil, Finney, and Vector76 attacks. This research adopts a systematic approach, which involves a comprehensive literature review, technical analysis of the attack mechanisms, and an evaluation of existing mitigation strategies. The study begins by outlining the fundamental concepts of these attacks, with a particular focus on how they exploit the decentralized nature of Bitcoin architecture. The technical breakdown of each attack is presented in detail, explaining how they operate and pinpointing the stages and components that enable these vulnerabilities. The paper illustrates the mechanisms behind the Sybil, Finney, and Vector76 attacks, providing a deeper understanding of their inner workings.

This is supported by detailed analysis and visual figures that map out the stages of each attack. The research is divided into several key stages. First, a thorough review of existing literature is conducted to gain insights into previous studies and methodologies. Following this, a technical analysis of Bitcoin network is performed, with a focus on identifying potential weaknesses in the transaction validation process, block propagation, and consensus formation. The study then introduces a visual pipeline figure that illustrates the transaction flow and identifies key points where each attack vector could intervene. This includes identity creation in the Sybil attack, pre-mining in the Finney attack, and timing manipulation in the Vector76 attack. Finally, the research assesses the effectiveness of current defense mechanisms and offers recommendations to strengthen Bitcoin network against these vulnerabilities. The flow of the study is depicted in Figure 1.

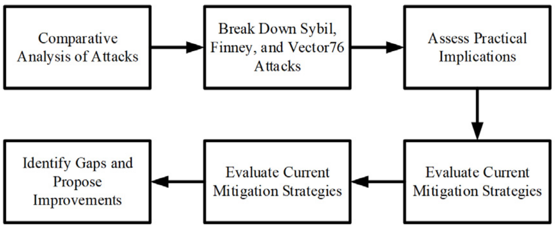
Comparative Analysis of Attacks
Break Down Sybil, Finney, and Vector76 Attacks
Assess Practical Implications
Evaluate Current Mitigation Strategies
Evaluate Current Mitigation Strategies
Identify Gaps and Propose Improvements

Figure 1: Research process (Picture credit: Original).

2.2 Attack Method

This study focusses on three prominent attacks in the Bitcoin network: Sybil, Finney, and Vector76. Posing significant risks to the network's security and integrity, each of the attack exploits different aspects of Bitcoin's consensus and transaction validation process. The Sybil attack is based on the principle of identity manipulation. In that case, a malicious actor creates multiple fake nodes to gain disproportion over the network (Douceur, 2002). Leading to potential disruptions in consensus and decision-making processes, the main concept of the Sybil attack is constructed by its ability of changing the system with the falsified identities. The primary characteristic of the Sybil attack is its scalability because a single attacker can create numerous identities with a low cost.

The Finney attack is an early double-spending attack which exploits the gap between block mining and transaction confirmation. In this attack, the adversary pre-mines a block which includes a transaction sending coins to themselves. Before broadcasting this pre-mined block, the attacker makes a transaction with the same coins to a different recipient (Karame, 2012). Once the second transaction is accepted, the pre-mined block is broadcast, invalidating the second transaction and effectively allowing double-spending. This attack highlights vulnerabilities in the transaction finality. The Vector76 attack combines elements of the race attack and the Finney attack. It relies on the timing between the block propagation and transaction confirmation. Once the attack handles the timing, it can exploit the double-spending vulnerability. Specifically, when the attacker sending a conflicting transaction to a merchant, the attacker broadcasts a valid block simultaneously. In that case, before the conflicting block invalidates it, the attacker can convince the merchant that the transaction is valid by manipulating the timing (Decker and Wattenhofer, 2014). The defining feature of the Vector76 attack is its reliance of precise timing manipulation, which offers a more sophisticated form of double-spending.

2.3 Defense Method

To counter these attacks on Bitcoin, several defense mechanisms have been proposed and implemented, each of them tailored to the specific characteristics of the Sybil, Finney, and Vector76 attack.

Against Sybil attacks, Bitcoin's PoW inherently offers some resistance by making it computationally expensive to generate multiple fake identities. Because of creating multiple identities requires significant computational resources, the cost of executing a successful Sybil attack becomes prohibitively high. Additional defenses include increasing node diversity and using reputation-based systems, where nodes gain influence based on trust or participation, rather than the number of identities.

For Finney attacks, the most effective countermeasure is increasing the number of required block confirmations before accepting a transaction as final. By waiting for multiple confirmations, merchants can reduce the risk of accepting a transaction that might later be invalidated by a pre-mined block. Some proposals also suggest using real-time transaction monitoring systems to detect anomalies associated with double-spending attempts. To prevent Vector76 attacks, improvements of the block propagation protocol, like the adoption of compact blocks or the fast block relay techniques, are able to minimize the time gap between block broadcast and confirmation. Furthermore, combining the transaction malleability combines with a more robust transaction verification processes can prevent attackers from manipulating the network's timing.

3 RESULT AND DISCUSSION

Generating fake nodes, the Sybil attack overwhelm the peer-to-peer network. One of its key strengths is the scalability, which means the more nodes the attacker can create, the more powerful the attack becomes. In that case, the scalability makes the Sybil attack particularly effective in the decentralized network. However, the Sybil attack has significant weaknesses. The main drawback is its reliance, which generates and maintains a large scale of fake nodes, which are resource-intensive when networks implement mechanisms like PoW or proof-of-stake (PoS) that require effort to maintain each node. Additionally, networks can defend against the Sybil attack by enforcing node reputation systems or limiting the number of new connections a node can make.

Enabling double-spending without the control of the significant portion of the network, the Finney attack exploits the vulnerability of unconfirmed transactions in Bitcoin. The advantages of this attack make the attack a relatively low-cost attack compared to others. However, the Finney attack is limited in the scope. Its effectiveness is highly dependent on the ability to pre-mine blocks and control transaction timing, making it less reliable. As a result, it is less likely to be widely effective in the network which owns high transaction volume or fast confirmation times. Additionally, requiring multiple confirmations for transactions effectively nullifies this attack, as it is only viable for transactions that are accepted after zero confirmations.

Combining aspects of the Finney attack with a race attack, the Vector76 attack is a more sophisticated method of double-spending. Its strength lies in its ability to exploit the timing differences between transaction broadcasting and block propagation. By broadcasting a transaction to a portion of the network while mining an alternate block that excludes this transaction, the attacker can reverse the original transaction when the alternate block is propagated. Nevertheless, because the Vector76 attack requires precise control over the transaction timing and the block propagation which makes it difficult to execute consistently, the complexity of the Vector76 attack is the weakness of itself. Furthermore, improvements in the network synchronization can significantly reduce the chances of success. Solutions such as reducing block propagation delay and requiring multiple confirmations reduce the effectiveness of this attack.

4 CONCLUSIONS

This research focused on analyzing three common Bitcoin attack methods: Sybil, Finney, and Vector76. Through a comprehensive approach, this study evaluated these attack vectors by examining their underlying mechanisms, success rates, and associated defensive measures. The analysis combined theoretical models with practical simulations to reveal the operational characteristics and real-world impacts of these attacks on blockchain networks. The experiments demonstrated both the vulnerabilities these attacks exploit and the limitations of current defense strategies. Moving forward, network synchronization will be a key area of research to enhance blockchain security. Future studies will emphasize improving block propagation speeds and developing real-time detection systems to more effectively counter these attack vectors. At the same time, efforts will focus on maintaining scalability and system performance, ensuring that increased security does not compromise the efficiency or robustness of blockchain networks. This research underscores the need for continuous advancements in both attack mitigation and system optimization to keep pace with evolving threats in the cryptocurrency ecosystem.

REFERENCES

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E.W. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In IEEE symposium on security and privacy, 104-121.

Decker, C., & Wattenhofer, R. 2014. Bitcoin transaction malleability and MtGox. In Computer Security-ESORICS European Symposium on Research in Computer Security, 313-326.

Douceur, J.R. 2002. The sybil attack. In International workshop on peer-to-peer systems, 251-260.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. 2016. On the security and performance of proof of work blockchains. In Proceedings of the ACM SIGSAC conference on computer and communications security, 3-16.

Hamdi, A., Fourati, L., & Ayed, S. 2024. Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: tools, analysis and countermeasures. International Journal of Information Security, 23(2), 713-757.

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. 2015. Eclipse attacks on Bitcoin's peer-to-peer network. In USENIX security symposium, 129-144.

Karame, G.O., Androulaki, E., & Capkun, S. 2012. Double-spending fast payments in bitcoin. In Proceedings of the ACM conference on Computer and communications security, 906-917.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.

Rosenfeld, M. 2014. Analysis of hashrate-based double spending. arXiv preprint:1402.2009.

Wen, Y., Lu, F., Liu, Y., & Huang, X. 2021. Attacks and countermeasures on blockchains: A survey from layering perspective. Computer Networks, 191, 107978.