Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/135/2025.21087

Security Challenges and Defense Strategies in Blockchain Systems

Xinyu Liang[1,a,*]

[1]Department of Information Science and Technology College, Dalian Maritime University, No. 1 Linghai Road, Dalian, Liaoning Province, China
a. liangxinyu@dlmu.edu.cn
**corresponding author*

Abstract: In the general use of blockchain technology, its decentralization, transparency, and immutability have demonstrated significant value in fields such as finance, logistics, healthcare, and public administration. However, this technology also faces a series of security and performance challenges. Especially in aspects of resisting malicious attacks, there is yet room for refinement. The integrated application of blockchain technology has gradually become an important driving force for new technological innovation and industrial transformation. Various industries have increased investment, research and development, and application landing of blockchain related technologies. The integration of blockchain technology with the real economy is accelerating. While blockchain technology and applications are rapidly developing, many industries are still in the exploration stage of blockchain applications. In the process of exploring the implementation of blockchain applications, obstacles to security risks have gradually emerged. Although blockchain provides reliable security guarantees at the underlying technology, attackers can still find security issues in the blockchain system and carry out attacks. The losses caused by network attacks are increasing year by year. This paper recalls the development and core principles of blockchain technology while focusing on major attack methods and summarizes the existing defense strategies against these threats.

Keywords: Blockchain, Security, Malicious Attacks, Defense Strategies

1. Introduction

As early as 1991, Haber and Stornetta came up with the timestamp-and-hash-based mechanism that could be used for verification in electronic documents. This is what laid the ground for some core ideas behind the blockchain technology. In 2008, Satoshi Nakamoto integrated this technology in the Bitcoin whitepaper and expanded it to build the first decentralized digital currency system by integrating the concept of a decentralized ledger and the Proof of Work mechanism. From there, the development of blockchain technology went from digital currency into decentralized autonomous organizations and decentralized applications, each time extending their field of application to finance, supply chain, and healthcare.

The core blockchain technologies are decentralized ledgers, cryptographic hash algorithms, and consensus mechanisms. The linking of blocks constitutes the chain, and each block basically consists of two parts: a block header and a block body. The block header metadata is defined with a version number, a hash of the previous block, a timestamp, the Merkle tree root, a nonce, and a difficulty target. These elements help in the verification of integrity within the block and achieve consensus among chain nodes. In the body, transaction data is stored as a Merkle tree for efficient verification of transactions. Blockchain allows for the distributed storage of data on the decentralized ledger and hence avoids a single point of failure, or security and transparency of data. It ensures data integrity and immutability through cryptographic hash algorithms; it achieves node consistency in a distributed environment by using consensus mechanisms.

Due to its characteristics, including decentralization, transparency, and irreversibility of recording, blockchain is considered one core driving technology among others for the onset of digitization. Having turned upside down the conceptual method of work, suggested methods for improving data safety and information openness for those traditional industries. Blockchain technologies with rapid development and expansion are gradually opening a number of security problems. Inadequate protection still exists in current blockchain systems. The study of the security problems of blockchain is not only of vital importance in improving its application prospects but also in accelerating its promotion in more extensive scenes.

This study is focused on analyzing the general attack principle and countermeasures that blockchain technology is facing and the exploration of possible future technological developments. Section 2 gives a brief overview of the basic principle of blockchain technology, common types of security attacks, and their defense methods. Section 3 tries to analyze the future development directions of blockchain technology and how to better enhance security and efficiency.

2. Security Challenges and Current Status of Blockchain Technology

Many of the attacks do not occur in isolation due to the diversity of attack methods and their scope of impact. Rather, many involve multiple domains or trigger chain reactions. In this paper, blockchain attacks are categorized based on their primary impact areas for clarity in discussion. They are: "communication attacks" against the links in communications, "consensus attacks" that manipulate consensus mechanisms for their vulnerabilities, "resource attacks" that disrupt services by depleting system resources, and "economic attacks" that attack blockchain incentive mechanism design flaws for improper economic benefits.

2.1. Communication Attacks

This type of attack manipulates the network paths or neighbor nodes in such a way that it blocks the target node from communicating normally with any other legal nodes or redirects the communications towards itself. By doing this, the attackers may tamper with the messages or even change some data sent in order to affect a target node in judgment over any transactions or state updates of the blockchain.

2.1.1. Eclipse Attack

The main reason for the occurrence of an eclipse attack is the existence of some kind of protocol vulnerabilities, especially in design-level P2P network connecting and node-selection mechanisms. With those weaknesses, an attacker can cut off the connections between the target node and the other nodes and connect the target through some nodes under its control. The victim node will only be able to exchange information with these malicious nodes controlled by the attacker. The data it receives will be fully under the attacker's control, and thus it will make biased judgments on confirmation outcomes.

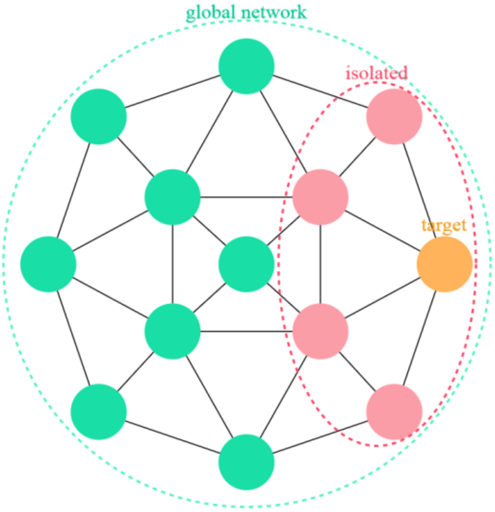

Figure 1: Eclipse Attack Diagram (Picture credit : Original.)

As shown in figure 1, in an Eclipse Attack, the victim node is completely surrounded and isolated by malicious nodes, blocking its communication with legitimate nodes.

Currently, widely adopted strategies include controlling the number of connections to target nodes and periodically removing inactive connections, as well as increasing the randomness and dynamic characteristics of connections to reduce the likelihood of communication being severed [1,2]. Further research has proposed several methods. These include a reference-based system for dynamically adjusting node trustworthiness by updating node behavior data in real-time and ensuring data integrity through distributed storage. This approach enhances the system's ability to precisely isolate malicious nodes while minimizing network performance degradation caused by attacks [2]. Another method involves extracting network traffic features from the Ethereum blockchain, utilizing multiple traffic characteristics (such as network entropy and packet communication statistics) to improve the detection accuracy of eclipse attacks. This approach enhances the recognition of anomalous patterns through multi-dimensional feature integration, optimizing detection efficiency [3]. Moreover, introducing a node mutual evaluation mechanism combined with the Kademlia algorithm strengthens dynamic defense capabilities, making node selection more reliable. This method reduces attack risks by implementing distributed computation and storage of rank values without modifying existing protocols, effectively minimizing the interference of malicious nodes while improving defense efficiency and system adaptability [4].

2.1.2. Routing Table Attack

To attack blockchain networks using dynamic routing protocols, an attacker connects to the targeted node and manipulates its routing table by injecting false routing information. A routing table coordinates the communication paths between nodes. Thus, in case of malicious changes in network information, a victim node may be misled to interact with malicious nodes controlled by an attacker, which can lead to possible information leakage.

The current enhanced defense strategies mainly include the optimization of routing table update strategies and enhanced scrutiny of a new node source to reduce malicious nodes entering a routing table. Further, multi-level routing verification can effectively avoid single-layer manipulation by an attacker in order to control data flow. These features of frequency limits and special conditions for routing table updates introduce dynamic connection update strategies, enabling higher accuracy of node selection and reducing the chance of malicious tampering with routing tables, hence improving the efficiency in resource use of the whole system [5].

2.1.3. EREBUS Attack

Factors such as vulnerabilities within smart contracts, protocol flaws, and a lack of efficient verification mechanisms caused the EREBUS attack. To compromise the target blockchain network, the attackers gradually take advantage of data flow management via manipulated Internet Service Providers (ISPs) and then widely distribute malicious autonomous systems across several ISP networks. By controlling the target nodes' main network paths and hijacking information in transmission to tamper with it. This type of attack can disrupt the blockchain's consensus mechanism.

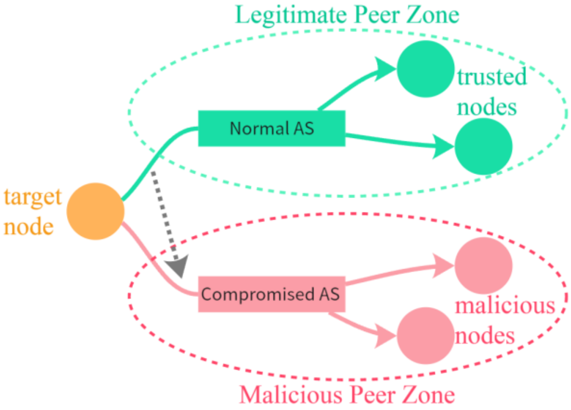

Figure 2: EREBUS Attack Diagram.(Picture credit : Original.)

As shown in figure 2, In an EREBUS Attack, malicious autonomous systems exploit vulnerabilities in the network by manipulating Internet Service Providers to control the flow of traffic to the victim node. The traffic from legitimate nodes intended for the victim node is intercepted and rerouted to a malicious AS, altering the original communication path.

Effective defense strategies against EREBUS attack include limiting the number of shadow IPs generated in order to reduce the chances of attackers occupying a large number of IP addresses [6]. By encouraging Bitcoin nodes to connect with more geographically dispersed peer nodes, reducing reliance on the same ISP paths will break the centralized control taken by attackers over network paths, which in turn reduces the attack success rate [1]. Recent studies have also introduced new defense approaches. For example, deep learning techniques that combine the multimodal features of traffic behavior and routing states to the use of feature selection methods that combine the ReliefF algorithm and WMRmR algorithm. In this way, redundant features can be effectively eliminated, the representation of features optimized, and the accuracy and stability of EREBUS attack detection improved [7]. Another proposed approach is to establish an integrated defense framework that features the RAP mechanism and adjustment of protocols, whereby the connection strategies are dynamically adjusted according to the network topology and geographic locations of Bitcoin nodes in an effort to effectively suppress the attack success rate in EREBUS attack [8].

2.2. Consensus Attacks

These attacks try to disrupt or hijack the consensus process of a blockchain system in order to change the state of certain transactions or data. In addition to posing threats to blockchain security, such an attack may also undermine the stability of decentralized networks.

2.2.1. % Attack

A 51% attack means that the attackers own the majority in a blockchain network, thus having the potential to control the computational power of the network. This might lead to tampering with data, blocking transactions, or even bringing down the whole blockchain network. Basically, the problem is caused by imperfect decentralization mechanisms, which permit a small group of miners to hold the majority of computing power.

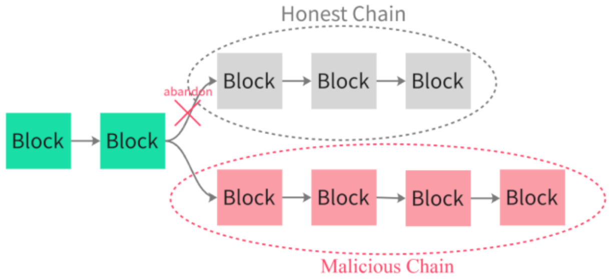

Figure 3: 51% Attack Diagram.(Picture credit : Original.)

As shown in figure 3, In a 51% attack, by leveraging superior computational power, the attacker extends their chain faster, eventually surpassing the length of the honest chain. When the attacker's chain becomes the longest, it is accepted by the network, rendering the honest chain invalid. This enables the attacker to rewrite transaction history, potentially leading to double-spending or other malicious outcomes.

The most common ways to alleviate 51% attacks are as follows. Increase decentralization of computational power by encouraging more small mining pools or individual miners to participate, which will avoid excessive concentration of computing power. Dynamically adjust the mining difficulty in accordance with the concentration of the network hash rate, reducing the possibility of a single mining pool dominating the entire network. Introduce multi-layered verification mechanisms to increase the cost and time it takes for an attack. Optimize network topology and enhance the diversity of node connections to improve network resilience and security [9]. Besides, resorting to the Delegated Proof of Work (dPoW) option enhances this security by timestamping blocks coming from a weaker blockchain onto a larger main chain; this effectively promotes resistance against attacks of the 51% style by introducing nodes that create checkpoints to avoid historic tampering with the blockchain. Yet, this scheme requires high computational resources, adding extra load into blockchain systems and hence might affect resource-constrained blockchain systems too much [10].

2.2.2. Double-Spending Attack

A double-spending attack is an incident where an attacker exploits delays in transaction confirmation to execute two different transactions with the same funds within a short period of time to commit fraud and obtain multiple services. The risk of such attacks lies in undermining the trust mechanism of the blockchain.

In order to prevent double-spending attacks, common strategies include lengthening the confirmation time of transactions to increase the cost of the attack, which would reduce the possibility of an attack being successful, and using a consensus mechanism with high consistency, such as PBFT, which guarantees node consensus before adding new blocks, avoiding chain fork risks in this way [11]. However, this may lead to problems of efficiency in high-frequency transaction scenarios. High-consistency consensus mechanisms normally set very high thresholds for node numbers and network conditions, which makes them unsuitable for highly decentralized networks. In light of these, some researchers propose an MSP framework. This framework processes transaction verification in several stages, including detection, confirmation, forwarding, and broadcasting, which reduces the possibility for attackers to utilize confirmation delays, thus reducing the success rate of a double-spending attack. The integration of multi-stage mechanisms with dynamic forwarding strategies strengthens defensive performance while keeping system operations stable [12].

2.2.3. Sybil Attack

In a Sybil attack, the attacking node creates multiple fake nodes to increase the influence in the blockchain network, create obstacles in consensus, and disturb the communication between the validating nodes. These fake nodes may intercept information flows, causing some legitimate nodes to fail to receive valid data and thus affecting system efficiency.

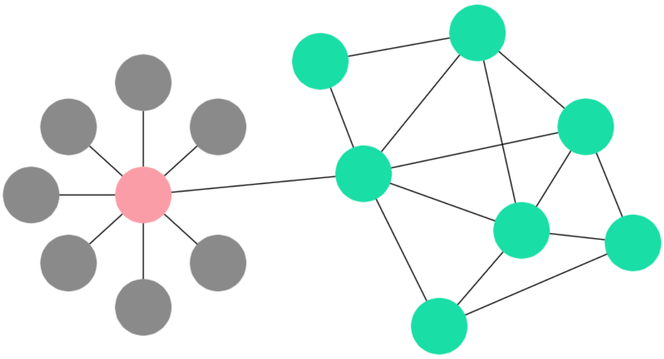

Figure 4: Sybil Attack Diagram.(Picture credit : Original.)

As shown in figure 4, These fake nodes, which were generated by attackers, interfere with communication and resource distribution, potentially isolating honest nodes or manipulating the network’s consensus.

Among common strategies to prevent such attacks are increasing the cost of creating nodes, such as Proof of Work (PoW) or Proof of Stake (PoS), in order to reduce an attacker's ability to generate fake nodes. Other strategies, like dynamic behavior monitoring and node verification mechanisms, trace the activities of the nodes and highlight unusual behavior with a view to reducing the potential influence of malicious nodes on the system. Further, several works suggest consensus protocols that combine randomness with reputation systems. The introduction of randomness in the election of leaders effectively inhibits attackers from predicting and compromising target nodes. The underlying reputation system dynamically adjusts a node's trustworthiness based on its historical behavior and hence constrains the long-term influence of fake identities [13]. Another approach is to design identity-enhanced PoS mechanisms that integrate identity authentication with reputation systems, which can ensure not only the reliability of node identities but also further suppress the creation of fake nodes [14].

2.3. Resource Attacks

It is an attack that tries to exhaust the computational power, storage capacity, or network bandwidth of a system to degrade its performance or even bring down the service and make it unavailable. One of the common ways to do this is through DDoS, where too much traffic is utilized to crash the system. A notable example is how the Ethereum network suffered from a DDoS attack via the vulnerabilities in its block reward mechanism. Attackers can flood the network with a very large amount of invalid transactions, which degrades its performance.

Effective DDoS mitigation strategies are fee- or time-based approaches for controlling mempool overload. The former requires transactions to pay relay and mining fees in an attempt to suppress spam or low-value transactions, while the latter introduces a "minimum age limit" into the mempool to exclude those low-value transactions [15]. Besides, it can adopt more efficient consensus mechanisms so as to enhance the processing capability of the whole system. The integration of blockchain with software-defined networking technology will enable dynamic traffic management and the implementation of security policies to timely detect and block malicious traffic [16].

2.4. Economic Attacks

Exploiting design flaws in blockchain incentive mechanisms, attackers use low-cost strategies to obtain undue profits. Such attacks compromise the fairness of the system, leading to an imbalance in the incentive mechanism.

2.4.1. Free-Riding Attack

Free-riding attacks take advantage of the nature of blockchain networks, where an attacker benefits from the computational effort of other nodes without contributing directly to the energy-intensive computations. In mining free-riding, attackers intervene when other miners are close to completing the mining process, securing rewards with minimal computational power. In transaction free-riding, attackers take advantage of others' efforts in transaction validation to reap transaction-related profits.

Some of the common measures of defense have been based on characteristics identified to restrain the contribution of the resources abusing users. Examples are lower service priority of such nodes, disconnection of a node, among others. Then there is also the possibility to adopt a P2P network model that is contribution-based, in which nodes obtain the services proportional to given contributions to a network. Contributory methods allow nodes to gain services either by paying money, being reciprocal, or for reputation. These mechanisms effectively incentivize nodes to actively participate in network activities, which enhances the stability and fairness of the system [5]. Further, another dynamic pricing model has been developed based on free-market mechanisms. By treating resources as commodities whose prices vary dynamically depending on supply and demand, along with their incentive mechanisms, this enhances efficiency in the fair allocation of resources and also effectively suppresses free-riding behavior [17].

2.4.2. Selfish Mining

Selfish mining is a process in which, after a miner successfully mines a new block, he does not broadcast it but instead continues mining to keep his lead. Once he has mined a number of blocks, he broadcasts them all at once. The blockchain protocols consider the longest chain as valid; hence, the blocks mined by other miners become orphaned and worthless. The root cause of selfish mining lies in the flaws of the reward mechanism. It acts unfairly toward the system by eluding other miners who deserve rewards from their work.

Optimizing the reward mechanism relies on tying the rewards with the block's publishing time, which can incentivize miners to broadcast a newly mined block immediately. Such measures decrease the withheld block's profit, which in turn minimizes the benefits derived from block withholding. Block propagation acceleration through better network protocols reduces the withheld nodes' time window for extending their chain, which in turn reduces the success rate of selfish mining. Other works propose the modification of the transaction data structure by including a "truth state" mechanism. Such techniques take advantage of a transaction's "expected confirmation height" parameter and some crucial blockchain system parameters for the detection of the presence of a selfish mining behavior during forked states. The network can thereby successfully identify and discard blocks mined by selfish miners [18].

3. Prospects for Blockchain Technology Development

The future development of blockchain should focus on integrating emerging technologies and optimization strategies to further enhance its security and efficiency.

3.1. Improvement Communication Attacks

Traditional methods of such attacks optimize the network topology and node connections to reduce attack paths. However, in dynamic environments and large-scale attacks, traditional methods are rather limited. For the identification of malicious nodes, most methods depend on fixed rules, which easily lead to the common problems of false positives and false negatives that weaken the defense effectiveness.

In recent years, more and more research has been focused on methods that are both intelligent and dynamic, studying behaviors or characteristics of nodes in different aspects combined with machine learning techniques to further improve the performance of malicious node detection. These methods overcome some traditional shortcomings but still need further optimization in terms of computational efficiency and real-time performance.

In view of the current limitations, multi-layer enhancement can be made in further research: develop better multi-tier defense models by integrating dynamic topology adjustment at the network layer with multi-level verification mechanisms at the protocol layer, improving the identification and interruption of complex attack paths; introduce real-time behavior analysis techniques at the application layer to improve the precision of anomaly detection.

Otherwise, adopting dynamic trust networks and smart contract technology during the optimization process of the limiting conditions of the cross-chain collaborative mechanism, which is conducive to prompting dynamic adjustment strategies of inter-chain data transmission and coordination of defensive strategies, rapidly constructing joint defensive systems on an extensive scale.

3.2. Improvement Consensus Attacks

Traditional methods of such attacks try to enhance system resilience through three ways: increasing decentralization in computational power distribution, optimizing the consensus process, and adding verification mechanisms. However, each faces many challenges during practical application. The high-consistency consensus mechanism often needs high node performance and good network conditions with limited dynamic adaptability. In a complicated network environment, there is still much room for improving the efficiency of attack detection and response.

In recent years, research has been done more and more on intelligent approaches. For example, some works have explored multi-stage verification frameworks that dynamically adjust strategies based on node behavior data and optimized verification processes using historical data. While these developments have enhanced the capabilities of defense, further optimization in resource efficiency and adaptability is required.

In this regard, future research work might focus on comprehensive and dynamic defense systems. First of all, in the design of the consensus mechanism, more flexible consensus strategies can be explored to integrate dynamic topology adjustment and distributed verification. This allows algorithms to adapt to different application scenarios while considering security and efficiency in a balanced way. It may be able to introduce randomness or identify enhanced strategies to reduce the possibility of attackers holding critical nodes in the selection mechanism of the consensus node. Most importantly, key attention can be paid to the practical usage of machine learning in the attack prediction and defense system. Through the training in node behavior analysis and historical data on transactions, it is possible to identify dynamic potential threats and make immediate changes in the strategy of defense; hence, responsiveness and adaptability increase.

3.3. Improvement Resource Attacks

Traditional defense methods against resource attacks optimize the enhancement of resource allocation, limit low-value transactions, and improve the efficiency of consensus mechanisms, which should be done in an attempt to minimize the impact of these kinds of attacks. In dealing with high-frequency, large-scale traffic attacks, these methods face great limitations due to their tendency to easily face performance bottlenecks. Second, most of the existing methods adopt static strategies that cannot quickly respond to dynamic traffic and ever-changing attack patterns.

To fix the shortcomings, the future research may take two routes: one is to develop more intelligent resource management strategies using machine learning algorithms for dynamic transaction traffic prediction and optimization of resource allocation; second, to investigate better collaboration models between blockchain and edge computing, where part of verification and computation tasks can be allocated to edge nodes for the purpose of alleviating the pressure on the main chain.

3.4. Improvement Economic Attacks

The defense against economic attacks depends on the optimization of blockchain incentive mechanisms to guarantee fairness and stability within the system. Future research can be devoted to more accurate and flexible economic strategies. First, a more complete multi-dimensional node contribution evaluation system can be explored. The system would take into consideration not only the computational power of nodes but also how often they participated, the quality of transactions produced, and past behavior, hence providing an integrated, more complete measure of a node's actual contribution to the network. The reward distribution mechanism would be designed to automatically adjust rewards according to the supply-demand relationship and network load conditions so that the elasticity of the incentive mechanism would be enhanced. Second, contribution records via smart contracts and distributed storage guarantee openness and transparency in rewarding distribution and, simultaneously, offer an environment to assure traceability of malicious behaviors, reducing illegal profit-seeking actions and strengthening system fairness.

4. Conclusion

This paper systematically reviewed blockchain technology and analyzed the principles and mechanisms of several attack types that blockchain systems can face, as well as existing defense strategies. Besides, based on the recent research developments, it proposes potential optimization directions.

In the future, further development of blockchain technology will focus more on the synergy of enhancing efficiency and security. On one hand, it is supposed that blockchain could support complex scenarios while accomplishing efficient operation by optimizing consensus algorithms, advancing cross-chain collaboration mechanisms, and exploring privacy-preserving computation technologies. On the other hand, the integration of dynamic defense technologies from AI and distributed systems will enable blockchain systems to solve potential threats proactively and precisely. Besides, the application scenarios of blockchain will be much more diversified and enriched with the increasing integration of blockchain with advanced technologies like IoT, edge computing, and AI. This will provide powerful technical support for the global digital transformation and the intelligent upgrading of social governance. No matter how promising the future, blockchain also takes more creative technology and more rigorous security guarantees.

References

[1] *Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1977-2008.*

[2] *Lin, L., Yiming, F., Tao, W., Haili, Z., Rongxin, M., Zhicheng, L., ... & Yvchi, X. (2023, October). Eclipse Attack Defense Method Based on Distributed Storage and Reference Value System. In 2023 IEEE 23rd International Conference on Communication Technology (ICCT) (pp. 1231-1236). IEEE.*

[3] *Bhumichai, D., & Benton, R. (2023, April). Feature Extraction of Network Traffic in Ethereum Blockchain Network Layer for Eclipse Attack Detection. In SoutheastCon 2023 (pp. 869-876). IEEE.*

[4] *Vinta, S. R., Patel, S. A., Sameen, A. Z., Soni, M., Khan, I. R., & Salman, H. M. (2024). Dynamic Defense Model against Eclipse Attacks in Proof-of-Work Blockchain Systems. Procedia Computer Science, 235, 1202-1212.*

[5] *Pradhan, S., Tripathy, S., & Nandi, S. (2018, December). Blockchain based security framework for P2P filesharing system. In 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.*

[6] *Tran, M., Choi, I., Moon, G. J., Vu, A. V., & Kang, M. S. (2020, May). A stealthier partitioning attack against bitcoin peer-to-peer network. In 2020 IEEE symposium on security and privacy (SP) (pp. 894-909). IEEE.*

[7] *Dai, Q., Zhang, B., Xu, K., & Dong, S. (2023). An Erebus Attack Detection Method Oriented to Blockchain Network Layer. Computers, Materials & Continua, 75(3).*

[8] *Tran, M., Shenoi, A., & Kang, M. S. (2021). On the {Routing-Aware} peering against {Network-Eclipse} attacks in bitcoin. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 1253-1270).*

[9] *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.*

[10] *Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied sciences, 9(9), 1788.*

[11] *Nasir, N. M., Hassan, S., & Zaini, K. M. (2024). Securing Permissioned Blockchain-based Systems: An Analysis on the Significance of Consensus Mechanisms. IEEE Access.*

[12] *Nicolas, K., & Wang, Y. (2019, October). A novel double spending attack countermeasure in blockchain. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0383-0388). IEEE.*

[13] *Platt, M., & McBurney, P. (2023). Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. Algorithms, 16(1), 34.*

[14] *Platt, M., & McBurney, P. (2021). Sybil attacks on identity-augmented Proof-of-Stake. Computer Networks, 199, 108424.*

[15] *Mrazek, K., Holton, B., Cathcart, C., Speirer, J., Do, J., & Mohd, T. K. (2022, May). Risks in Blockchain–A Survey about Recent Attacks with Mitigation Methods and Solutions for Overall. In 2022 IEEE International Conference on Electro Information Technology (eIT) (pp. 5-10). IEEE.*

[16] *Giri, N., Jaisinghani, R., Kriplani, R., Ramrakhyani, T., & Bhatia, V. (2019, December). Distributed denial of service (DDoS) mitigation in software defined network using blockchain. In 2019 third international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) (pp. 673-678). IEEE.*

[17] *Kurdi, H., Althnian, A., Abdulghani, M., & Alkharji, S. (2020). An Adjusted Free-Market-Inspired Approach to Mitigate Free-Riding Behavior in Peer-to-Peer Fog Computing. Electronics, 9(12), 2027.*

[18] *Saad, M., Njilla, L., Kamhoua, C., & Mohaisen, A. (2019, February). Countering selfish mining in blockchains. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 360-364). IEEE.*