Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/49/20241130

Investigating and mitigating blockchain poisoning attacks

Haoyu Hu

Computer Institute, University of West Scotland, Glasgow, PA1 2LH, Scotland

B01655369@studentmail.uws.ac.uk

Abstract. With the burgeoning adoption of smart contracts and the intrinsic anonymity that blockchain technology provides, the past few years have witnessed an exponential surge in the deployment of blockchain platforms for managing crypto assets. While Ether stands as a paragon of blockchains equipped with smart contract capabilities, it's noteworthy to mention that such blockchains present a blank canvas in the form of a data list, dedicated for unbridled program storage. This vacant space, though pivotal for various operations, can become a potential Achilles' heel. Specifically, if this repository gets tainted with malicious data, the repercussions can reverberate across the entire blockchain, disrupting its core functions. The research in focus shines a spotlight on a particularly insidious threat, termed 'blockchain poisoning attack.' Through this stratagem, malevolent actors can, with minimal expense, embed detrimental files within the data space, thereby extensively polluting the blockchain. This isn't just a theoretical hazard; its practical implications are stark and can jeopardize the integrity of countless transactions. In a commendable feat of investigative rigor, the research meticulously decoded the modus operandi behind these blockchain poisoning attacks. By employing a multi-pronged research approach, encompassing in-depth studies and iterative inquiries, it successfully deconstructed the exact techniques that malefactors employ.

Keywords: Blockchain, Defense, Attack, Smart Contract, Poisoning.

1. Introduction

While blockchain stands as the linchpin behind cryptocurrencies or cryptographic assets, it's more than just a vehicle for digital currencies. As a distributed ledger, blockchain offers compelling advantages for commercial applications and safeguarding cryptographic data. Its design ensures network continuity, a semblance of privacy, and resilience against data tampering. Yet, as technological advancements surge forward and an array of sophisticated hacking techniques emerge, blockchain confronts a slew of security quandaries and challenges. The technology isn't just grappling with well-documented threats like the 51% attack, double-spending attacks, and cryptojacking but also with newer threats like the 'poisoning attack' illustrated subsequently.

A poisoning attack on a blockchain transpires when malevolent actors embed malicious or illicit files within the blockchain's data space. This form of assault isn't just an ordinary cyber threat. Its ramifications are more sinister than conventional poisoning attacks on public databases, such as DNS cache poisoning. Given blockchain's inherent design — where transactions, once entered, are immutable and cannot be altered or annulled without instigating a major protocol change (a hard fork) — rectifying a poisoned blockchain becomes a daunting task. Compounding this issue is the distributed nature of the blockchain, where data is synchronized across all participating nodes. This means an attacker, after

DOI: 10.54254/2755-2721/49/20241130

compromising a single node, can potentially sully the entire blockchain, coercing other nodes into downloading deleterious files.

Ether, the lifeblood of the Ethereum platform, epitomizes the full realization of a smart contract system. Distinct from the more rigid structure of Bitcoin's blockchain, Ethereum offers a malleable space housing the bytecode of smart contracts. This versatility, while advantageous, also presents vulnerabilities. Given Ethereum's accommodating nature, embedding data into its blockchain becomes a straightforward affair for anyone, malefactor or otherwise. This ease of data insertion grants attackers unprecedented latitude, making platforms like Ethereum susceptible to attacks, especially the aforementioned poisoning. Given these circumstances, poisoning attacks are emerging as a looming menace, especially for platforms as open-ended as Ethereum. As shown in Figure 1.

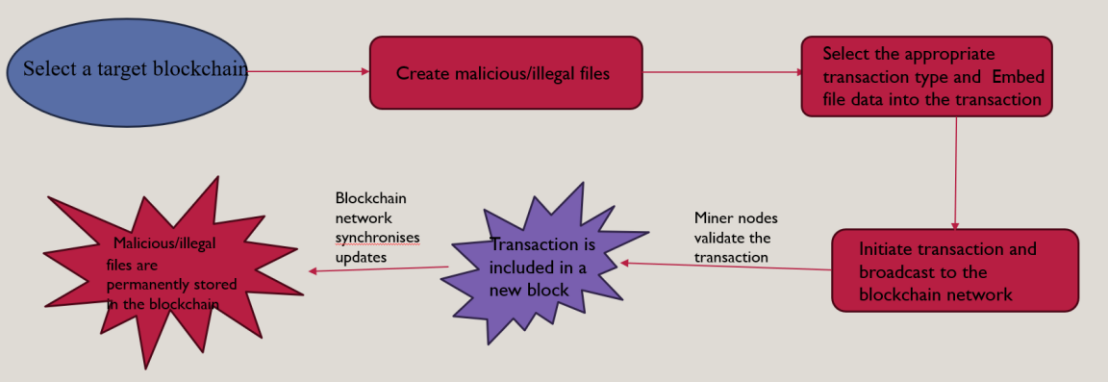

Figure 1. Structure diagram (Photo/Picture credit: Original).

2. Literature Review

2.1. Overview of Security Threats in Blockchain

With the advancement of blockchain technology comes widespread attacks and more publicised risks. These attacks or risks may be due to internal participants or external entities. The growing popularity of blockchain has created new privacy and security concerns for data transmission and storage [1]. The current blockchain security threats can be broadly categorised as double spending threats, most of the attacks (51% attack), cryptojacking, as well as a poisoning attack. These categories have different characteristics in terms of attack methods and threatening nature, but all threats to the blockchain must be taken seriously.

Double spend threats:An attacker has the ability to pay a merchant, acquire the products or services, and then transfer the remaining funds to an account that is either his own or that of another merchant [2]. Since the account message and the original message conflict with each other, if the secondary consumption message, rather than the original message, is confirmed by the consensus system, the buyer will withdraw the payment, but the merchant will not receive payment for its goods [3].

51% threats:In a 51% attack, a malicious entity or group of miners gains control over more than 50% of the total computational power (hashrate) of the network. When they have this majority control, they can manipulate the blockchain in various ways, including:

Double Spending: The attacker can spend their cryptocurrency coins and then create an alternative version of the blockchain where those spent coins are not recorded [4]. This allows them to spend the same coins again, essentially "double-spending."

Blockchain Reorganization: With majority control, the attacker can create a longer blockchain fork (alternative blockchain) than the existing one. This longer chain may contain different transactions, and if accepted by the network, it replaces the original chain [5], causing a reorganization of the blockchain.

Censorship or Denial of Service: An attacker with majority control can choose to include or exclude specific transactions from the blockchain, effectively censoring transactions or preventing certain users from conducting transactions.

DOI: 10.54254/2755-2721/49/20241130

It's important to note that conducting a 51% attack is an expensive and challenging task, as it requires a significant amount of computational power and resources to overpower the honest miners in the network. In well-established blockchains like Bitcoin, the cost of executing such an attack is extremely high, making it less likely.

Cryptojacking threats:Cryptojacking or illegal mining is a type of malware targeting the blockchain, which usually hides in the victim's computer and uses computational resources to extract cryptocurrency in favour of the attacker. It also reduces the computational efficiency of the victim's computer as it generates a large amount of computational consumption.

2.2. Definition of Blockchain Poisoning Attacks

An assault on a blockchain is known as a "blockchain poisoning attack," which involves inserting harmful or unauthorised files into the flexible space of the network. A DoS attack on the blockchain can be launched by an attacker by compelling a node in the network to download the file. The blockchain and its users may be the attack's target [6]. The attacker carries out the assault as follows:

Attacker first creates harmful or unlawful files; then attacker embeds file in adaptable transaction area and publishes transaction on blockchain network; After being mined into the blockchain, the malicious file is distributed across network users.

2.3. Examination of Specific Case Studies

In order to determine how and what to attack, the first step is to programme the programmable space

Conducted research on the primary Ethernet network's programmable space [7].

Detection of transaction-embedded files by the file carving method. This method operates in such a way that it is used to recover files from unallocated space in storage. In digital forensics. It identifies the files embedded in unknown binary data by techniques such as searching the file header and using the file structure, after identifying it, the format of the file with the exact number of files can be obtained. Foremost is used in this evaluation as it can be used in both generic and open source programes.

The investigation procedure is as follows:

1. convert the data extracted from the transaction from a byte array to a binary file and then save the file.
2. feed the binary file into the file carving tool.
3. if the tool detects certain files in the binary file, record the transaction information.

The following chart shows the data obtained from the survey:

DOI: 10.54254/2755-2721/49/20241130

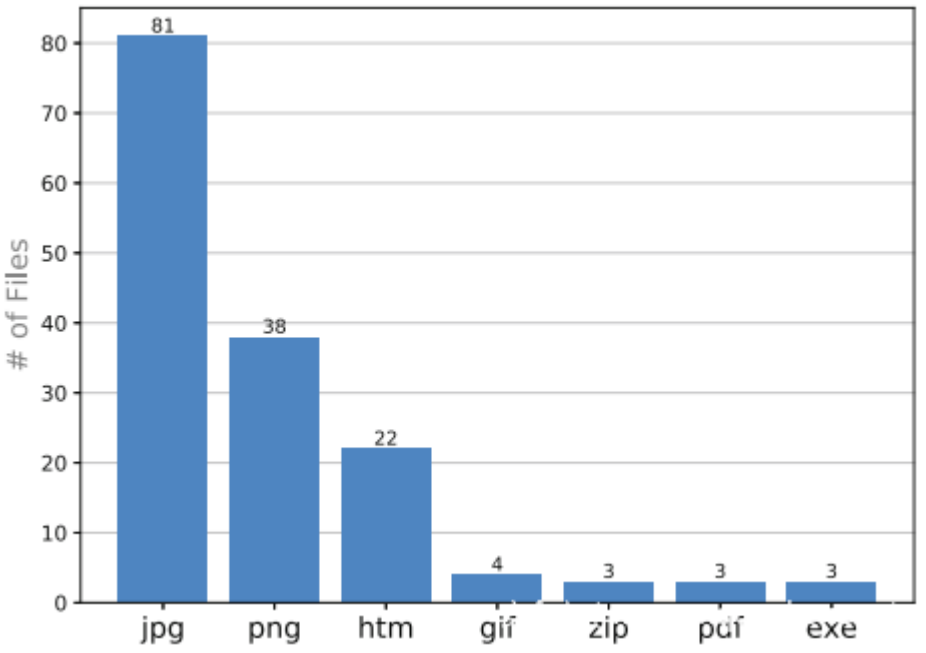

Figure 2. Data distribution (Photo/Picture credit: Original).

154 files were discovered to be contained in the Ether blockchain, according to an analysis of the data taken from the transactions. The file types of the extracted files are displayed in Figure 2. According to the graph, image files (jpg, png, and gif) make up around 80% of the extracted files [8]. Because they are landscapes and group shots, the majority of the image contents are not objectionable. However, some photos include offensive material. Additionally, even seemingly innocent photos might be dangerous since they could breach the privacy of others or exploit steganography to their advantage. The Ether blockchain contained three exe files.

The MD5 hashes of these three exe files are shown below;

(1) c9a31ea148232b201fe7cb7db5c75f5e.

(2) c1e5dae72a51a7b7219346c4a360d867.

(3) c9a31ea148232b201fe7cb7db5c75f5e.

These two files are obviously identical. These hashes were entered into VirusTotal to evaluate the files and it was concluded that the three exe files were malware as the analysis of files (1) and (3) showed that they were detected by anti-virus software at a rate of 56/70 and the results for file (2) showed that it was detected at a rate of 58/66. According to the report, a type of malware called W32. A malware named "W32.Duqu" has the same hash values as files (1) and (3).

In addition, it was found that the three exe files were embedded by an account that sent three transactions with embedded files in about six minutes. The following figure shows the time series histogram of the transactions of the embedded files [9]. As shown in Figure 3.

DOI: 10.54254/2755-2721/49/20241130

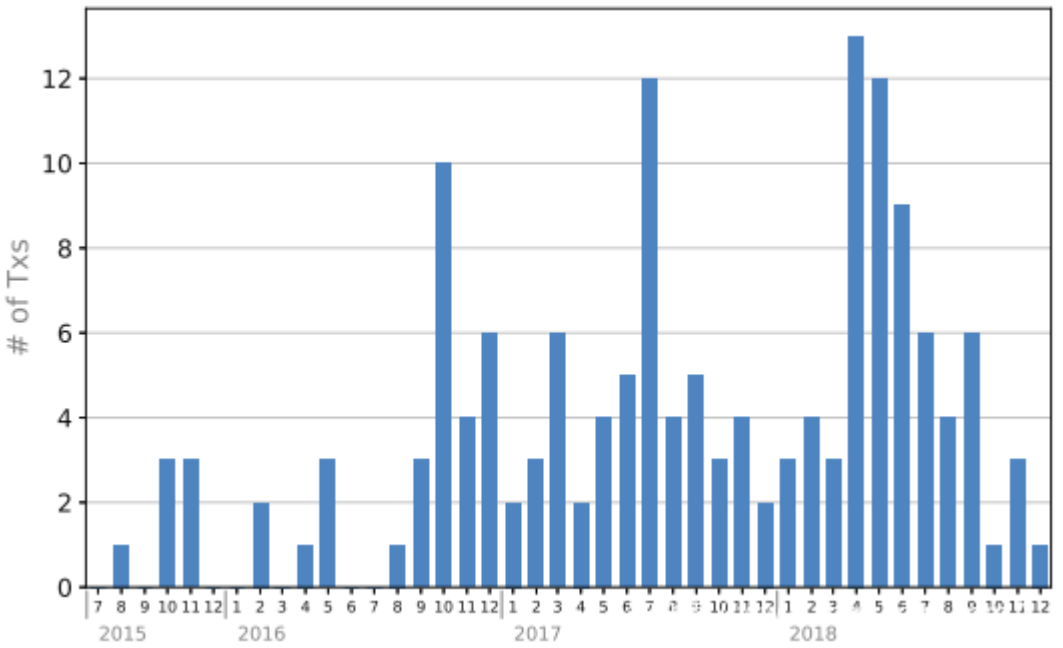

Figure 3. Year change chart (Photo/Picture credit: Original).

The following illustration shows a time-series histogram of transactions embedded in a file, demonstrating the relationship between the sender and receiver of an embedded file for a transaction. 113 sender accounts and 154 transactions with files embedded are present. This suggests that some accounts have placed files on the Ethereum blockchain several times. A single account may send a maximum of 10 file embedding transactions.

Table 1. Transaction Types Based on Sender and Recipient in Blockchain.

Sender and recipient are the same	79
Sender and recipient are the different	70
Recipient is null (contract creation transacition)	5

The number of connections between the sender's and the recipient's accounts is shown in the Table 1 above. There are three main kinds of relationships: (a) when the sender and receiver are the same; (b) where the sender and recipient are different; and (c) where the recipient is null (i.e., where the transaction is created by the contract). The majority of accounts with transactions that include files send the transaction to a receiver other than null. Several accounts include transactions for contract formation that include files [10].

Poisoning Attack Feasibility Experiment.

After obtaining this data, experiments need to be constructed to test the poisoning attack, requiring the following environment:

Server A (Ethernet Private Network): On this server, which is set up to mine private blockchains, Go Ethereum is installed. In a real-world setting, this server assumes the function of the primary Ether Net.

Server B (Explorer): On this server, a web server is configured to show data from Server A's Ether private blockchain using Eth Explorer. In a real-world setting, this web server simulates a blockchain browser like Ether scan.

Laptop: shell commands were executed using a laptop and experiments were conducted using Google Chrome (with METAMASK installed). These enable the same process of embedding and extracting files as a poisoning attack on the main Ethercan network.

The specific flow of the experiment is as shown in Figure 4.

DOI: 10.54254/2755-2721/49/20241130

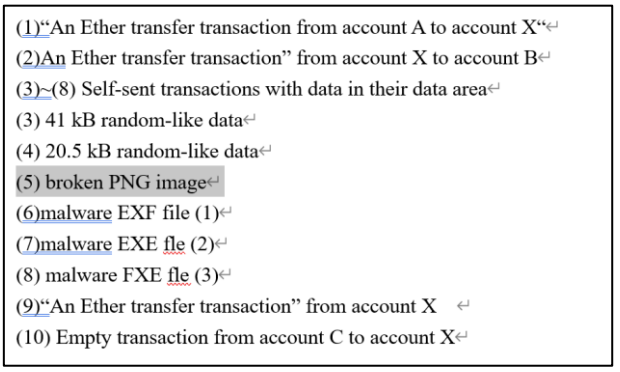

Figure 4. Steps of the experimental process (Photo/Picture credit: Original).

The experiment is divided into three steps: preparation, embedding and extraction of files, and the following Figure 5 shows the flow of the experiment.

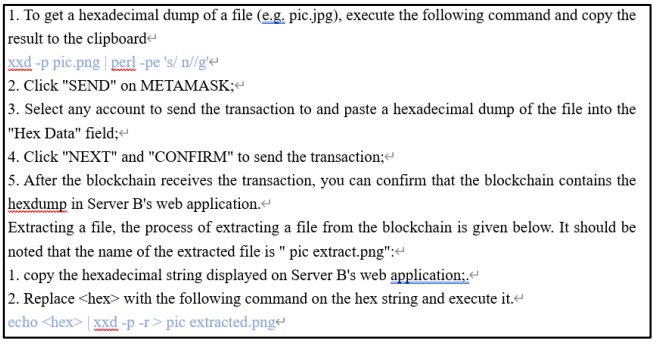

Figure 5. Experimental process (Photo/Picture credit: Original).

In the experiment, the behaviour of the suspicious account was observed by a single account that could embed three exe files (malware) into the Ethernet blockchain and analyse the malware for suspicious behaviour. These transactions were as follows. It is assumed that "X" represents the unsettling tale and accounts A, B, C represent regular accounts.

This series of transactions shows an attacker trying to check if a malicious file can be embedded in the blockchain. This series of transactions suggests that the attacker is trying to check whether malicious files can be embedded in the blockchain, and the experiment detected suspicious behaviour through one account. However, it's clear that distinction between malware and such suspicious accounts, so heuristic analysis of each account is ineffective due to the differences between malware and accounts on the blockchain,.And instead of focusing on the account, precautions against blockchain poisoning should be done by examining each transaction.

3. Analysis Blockchain Poisoning Attacks

3.1. Underlying Mechanisms of the Attacks

According to the survey, blockchain poisoning attacks may occur with the following attack mechanisms.

Transaction Rejection Attacks and Mechanisms: interferes with the normal functioning of the blockchain by sending malicious transactions into the blockchain which may cause network congestion or node crashes when processed by the blockchain.

Suspended Transaction Attacks: by sending invalid or malicious transactions, even if these transactions look legitimate, they will be rejected by the contract later in the block, as the transactions are rejected, the time and computational resources of the other participants are wasted to validate these transactions, and the efficiency of the network will be reduced as a result.

DOI: 10.54254/2755-2721/49/20241130

Malicious Smart Contracts: by deploying malicious smart contracts on the blockchain, these malicious contracts enter the chain, e.g., to steal funds, tamper with data, or trigger other actions detrimental to the network.

Infinite Loop Attacks: by creating smart contracts with infinite loops that force network nodes to perform certain operations indefinitely, thereby causing network congestion, to achieve the attack.

3.2. Motivations Behind the Attacks

The motivation for a blockchain poisoning attack can be varied, depending largely on the goals of the attacker. Through research, here are some of the main motives that may give rise to a blockchain poisoning attack.

Financial Benefit: Attackers are mainly likely to try to gain financial benefits through poisoning attacks. They can embed malicious information in the blockchain by poisoning it, which is likely to allow the attacker to profit from the victim's proceeds.

Competitive advantage: some attackers may belong to a competing cryptocurrency project or team and, in order to gain a competitive lead, try to attack a competitor's blockchain through a poisoning attack to gain a competitive advantage or undermine the competitor's credibility.

Revenge or Malice: Some attackers may be motivated by personal revenge or malice in an attempt to undermine a specific blockchain project or to take revenge on a specific individual or organisation.

Knowledge testing and vulnerability detection: some security researchers may perform poisoning attacks to study the vulnerabilities of blockchain technology and provide solutions to strengthen its security. It may also be used to test the weaknesses and vulnerabilities of blockchain systems to improve their security.

3.3. Consequences and Risks

Network instability: Poisoning attacks may result in node failures, transaction delays, and network congestion. The blockchain's performance and accessibility suffer as a result.

User distrust might be damaged by a successful poisoning attack, leading users to question the blockchain's dependability and security. Users could then withdraw their money and switch to other blockchains or systems as a result of this.

Economic damages might result from poisoning assaults if bitcoin holdings are stolen or destroyed. Attackers may make money by robbing people or causing market instability.

Network forks: If an assault is successful, it may result in a network fork that enables various nodes to operate on distinct branches of the blockchain. As a result, the network becomes more complicated and may become inconsistent.

Legal Liability: Blockchain poisoning attacks are typically prohibited, and perpetrators may be subject to civil lawsuits as well as criminal prosecution. The attacker's personal and professional lives may suffer as a result.

Poisoning attacks may harm the whole blockchain ecosystem, including projects, developers, investors, and users. This would prevent the ecosystem's expansion and development.

Reputational damage: Poisoning assaults have the potential to harm a blockchain project's reputation, which would erode user and investor confidence and lower the project's market value and sustainability.

4. Countermeasures Against Blockchain Poisoning Attacks

4.1. Detection Techniques and Alert Mechanisms

Detection Techniques.

In the current mainstream blockchain, many targeted detection methods and alarm mechanisms have been developed to cope with and detect poisoning attacks.

The first is abnormal transaction detection, blockchain through the detection of real-time monitoring of transactions on the blockchain, to identify abnormal transaction behaviour, such as large transfers,

DOI: 10.54254/2755-2721/49/20241130

frequent transactions and so on. Usually this detection method is built on transaction patterns and pre-set rules.

There is also the tagging of already existing addresses and the creation of labels for malicious addresses to be able to track transaction activity related to these addresses.

And with the development of cloud computing and big data, the use of big data technology to analyse blockchain data in order to detect unusual patterns or trends is also gradually becoming a viable means.

And the use of artificial intelligence to build machine learning models to monitor transactions and contract execution for anomalous behaviour is also coming into use. These models can be trained on targeted data to identify new patterns of poisoning attacks.

And on the network side, by detecting network activity in real time to detect any unusual network traffic or node behaviour.

Alerting Mechanisms.

And now the alarm mechanism of blockchain mainly has real-time alarm, that is, through the establishment of a tethered smart contract or system to monitor the activities of the blockchain in real time, and immediately notify the relevant personnel in the event of any abnormality. Meanwhile the relevant anomaly report will be recorded in the event log for reviewing and analysing afterwards.

4.2. Defensive Strategies

Since Ether has a legitimate and flexible space, any participant in a transaction can embed data in the flexible space of the Ether blockchain. And this feature not only facilitates ease of transactions, but also provides flexibility for attackers. As a result, poisoning Ether (and blockchains with flexible spaces) is easier, and in order to keep users safe, it is necessary to understand the relevant means of defending against poisoning attacks.

Through this given experiment, more about the scope and manner of poisoning attacks are recognised, which also helps in making modifications to smart contracts to defend against attacks.

Data validation and filtering: Strict validation and filtering of data received from external sources is always performed in the contract. The type, scope and format of the input data are validated to prevent incoming malicious data.

Contract isolation: If you need to store user uploaded files or data in a contract, consider using an isolated storage contract to ensure that user data does not compromise the security of the main contract. Of course, adding a sandbox environment to the contract is also a viable option.

Minimal storage and manipulation: Store and manipulate only the minimum data required by the contract. Avoid storing too much unnecessary data, thereby reducing the attack surface.

4.3. Case Studies of Successful Defenses

Case description: Ethereum 2.0: Ethereum 2.0 is considered to be the next-generation version of Ether, which defends against and responds to blockchain poisoning attacks by upgrading a more reliable and security-assured consensus mechanism. Since Ether 1.0 had been attacked multiple times, Ethereum 2.0 was designed to improve the network's security and resistance to attacks.

Key Defence strategies: Firstly the new Proof of Stake (PoS) consensus algorithm was creatively adopted to reduce the influence of miners on blockchain transactions and reduce the possibility of attacks. Secondly, the introduction of slicing technology, which divides the network into multiple segments, ensures that even if the blockchain is attacked, the threat is kept within acceptable limits, reducing the risk of an attack on the entire network.

Finally, the security of the blockchain in Ether is further improved by improving the logic and functionality of smart contracts, achieving the goal of reducing vulnerabilities.

DOI: 10.54254/2755-2721/49/20241130

5. Enhancing Defensive Measures

5.1. Challenges in Fortifying Defenses

In the face of technological advancement and the adoption of more and more innovative technologies, the security of block practice is also facing greater challenges.

First of all, there are more and more new attack techniques. In order to achieve their goals, attackers will do their best to update their attack techniques to cope with the defence means, which also puts greater demands on the work of the defenders.

Secondly, because smart contracts are automatically executed code on the blockchain, they often have vulnerabilities. These vulnerabilities can lead to loss of funds or improper execution of contracts. And while auditing and testing smart contracts can become critical, a slip-up can be devastating

Third, attackers won't just rely on technical vulnerabilities, but will also trick users into providing private keys or login credentials. Such phishing attacks must also be popularised and users must be wary of them.

5.2. Directions for Future Research in Targeted Countermeasures

For enhanced defense against poisoning attacks, future research might consider delving into the following avenues:

Sophisticated Attack Detection Logic: Enriching the contract with advanced attack detection mechanisms, which could involve identifying specific malicious data patterns or recognizing suspicious behaviors.

External Service Integration: Leveraging third-party services to validate external data could be instrumental. Such integrations would not only corroborate the authenticity of the data but also help in spotting anomalies.

Hierarchical Alert System: Establishing a multi-tiered alert system could be pivotal. This would allow the contract to issue alerts based on the gravity of the perceived threat. Additionally, tailoring specific remedial actions corresponding to each alert level could amplify the response efficacy.

Granular Event Feedback: In instances where an alert event is initiated, the contract might be designed to retroactively furnish comprehensive details, like the probable attacker's address, the nature of the assault, and so forth. However, discerning whether such an activity indeed constitutes a breach remains a matter of debate.

Proactive Response Mechanism: Incorporating an automated response function within the contract could be transformative. In scenarios where an attack is perceived, this mechanism would autonomously halt or pause contract functionalities, ensuring potential damages are mitigated with optimal swiftness.

By charting research along these lines, one could significantly bolster the resilience of blockchain systems against poisoning attacks, making them more robust and dependable in an increasingly complex threat landscape.

6. Conclusions

This exploration delves deep into the intricacies of blockchain poisoning attacks, commencing with an elucidation of their definition and the requisite conditions for their execution. The examination gains depth as it ventures into an analytical study of programmable spaces within the Ethereum network, further underscored by an empirical feasibility assessment to delineate the nuances of such attacks on blockchain ecosystems. In the labyrinth of digital ledger technology, the peril of blockchain poisoning attacks looms large. These assaults, with their distinctive threats, operational methodologies, and assault mechanisms, have profound implications. This treatise methodically unravels these multifaceted aspects, shedding light on the ramifications of such breaches. It's not merely about identifying vulnerabilities; it's about understanding the ramifications that ripple across networks, stakeholders, and end-users. Furthermore, in an age where proactive defense is as crucial as retrospective mitigation, this work doesn't halt at merely delineating the problem. It offers a comprehensive overview of potential defensive strategies, illuminating pathways that not only neutralize current threats but also bolster resilience

DOI: 10.54254/2755-2721/49/20241130

against future incursions. The discourse culminates with a forward-looking perspective, charting out trends and trajectories that could shape the evolution of blockchain security in the coming years. In essence, this piece stands as a holistic tableau, presenting a sweeping view of poisoning attacks in the realm of blockchain. It aspires to bridge knowledge gaps, inform stakeholders, and catalyze informed strategies to fortify digital assets against looming cyber threats.

References

[1] Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Computers & Electrical Engineering,(Volume 90)

[2] Li, Y., & Wang, C.-C. (2022). A search-theoretic model of double-spending fraud. Journal of Economic Dynamics and Control, (Volume 142)

[3] Aponte-Novoa, F. A., Álvarez, D. P., Villanueva-Polanco, R., Orozco, A. L. S., & García Villalba, L. J. (2022). On Detecting Cryptojacking on Websites: Revisiting the Use of Classifiers. Sensors,

[4] Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16).

[5] Conti, M., Jäschke, A., Lal, C., & Spagnuolo, M. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.

[6] Admin. (2023). Threat Analysis of Poisoning Attacks in Ethernet Blockchain. https://www.ctfiot.com/94895.

[7] Sharma, D. K., Pant, S., Sharma, M., & Brahmachari, S. (2020). Chapter 13 Cryptocurrency Mechanisms for Blockchains: Models, Characteristics, Challenges, and Applications. Handbook of Research on Blockchain Technology (P349-P371),Elsevier.

[8] Steiner-Otoo, D., & Jahankhani, H. (2022). An Investigation into How Smartphones Can Be Secured Against MiTM Attacks: Financial Sector. In Blockchain and Other Emerging Technologies for Digital Business Strategies (pp. 171-215). Cham: Springer International Publishing.

[9] Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, (Volume 50),4.1. Elsevier.

[10] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence Computing, (Volume 2), Elsevier.