International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I4P101

Volume 72 Issue 4, 1-14, April 2024

Original Article

Blockchain and Cryptocurrency Security from a New Layered Perspective and a Novel MITRE ATT&CK-based Approach for Understanding Cyberattacks and Mitigating Their Impacts

Sara BARJ[1], Abdellah YOUJIL[2]

[1]*RAISS Team, STRS Lab., CEDOC 2TI, National Institute of Posts and Telecommunications, Rabat, Morocco.*
[2]*General Directorate of Information Systems Security, Rabat, Morocco.*

[1]*Corresponding Author : sara.inpt@gmail.com*

Received: 14 November 2023 Revised: 10 April 2024 Accepted: 11 April 2024 Published: 24 April 2024

Abstract *- This paper comprehensively examines cyberattacks targeting blockchain networks and systems, inspects attacks at different blockchain layers, and adapts MITRE ATT&CK concepts to the blockchain and cryptocurrency context. It identifies the most common attack methods used by cybercriminals. This research underscores that attacks can occur at various layers of the blockchain, including the Data, Consensus, Execution, and Application layers, which implies the importance of understanding the different layers of the blockchain and the potential security risks associated with each layer. The findings stress that no single layer is immune to cyberattacks, and each requires a distinctive approach to secure blockchain platforms. By defining prominent cyberattacks on the blockchain, this paper analyzes cyberattacks and their related recommendations for enhancing the security of the blockchain platform from a layered perspective and MITRE ATT&CK approach. These recommendations include robust consensus protocol selection, secure coding, regularly executing updates, using protection tools, and social engineering sensibilization. Furthermore, this paper highlights the pivotal role of developers and industry professionals in prioritizing the platform's security throughout the entire development lifecycle to prevent potential security risks. Finally, this work's recommendations aim to empower developers and industry professionals to secure their Blockchain systems against cyberattacks, thereby enhancing the security and reliability of blockchain technology.*

Keywords *- Blockchain technologies, Blockchain layers, Cyberattacks, Cybersecurity, DCEA framework, Distributed systems, MITRE ATT&CK framework, Security recommendations.*

1. Introduction

Blockchain technology is revolutionizing data management and storage. It offers secure and decentralized platforms for transactions and information exchange. However, as Blockchain-based systems become more prevalent in various industries, the need for robust security measures to protect from cyberattacks and sensitive information leakage becomes increasingly important. Indeed, the potential consequences of cyberattacks on Blockchain systems, such as data breaches and financial losses, underscore the urgency of understanding the layers of Blockchain technology and the types of attacks that can occur at each of them to create effective security measures. In this direction, this work addresses the following problem novelly: How can a blockchain platform be effectively designed and secured through a layered perspective or MITRE ATT&CK approach? To address this paper's research problem, it explores blockchain security while understanding the surveyed cyberattacks and focusing on a layered approach and MITRE ATT&CK concepts [1] for proposing adequate measures to mitigate their impacts and severity. The chosen DCEA framework [2] has many benefits, like presenting the main Blockchain layers, focusing on the blockchain system, and ignoring the network layer.

Besides, we choose the MITRE ATT&CK framework for its ability to help organizations understand the full spectrum of potential threats they may face, and it is the first time in the literature that it has been adapted to Blockchain platforms. This work provides definitions of attacks, which help to identify the targeted DCEA layers and to conclude recommendations for defending the blockchain against these attacks, which permits the achievement of this research paper's goals.

The second section surveys and defines the various attacks targeting Blockchain systems. The third section describes the materials and methods used in the study, including the presentation of the DCEA framework, the targets of the surveyed cyberattacks related to Blockchain networks and systems, and the proposed process to adapt the MITRE ATT&CK concept to the Blockchain context.

The fourth section reveals the study's findings and results, including identifying the Blockchain layers targeted by Blockchain attacks and presenting the main recommendations for securing blockchain networks and systems against the attacks identified in the study.

In addition, it proposes a new simplified MITRE ATT&CK framework for the Blockchain and Cryptocurrency context and its application to the real world. Finally, the last section concludes this paper and provides future directions.

2. Background: Attack Definitions

As the popularity of Blockchain systems evolves, so do the requirements to secure and defend them against cyberattacks. Many attacks can target Blockchains, each with its methods, objectives, and targets. This section briefly defines the surveyed attacks affecting Blockchains.

2.1. A Double-Spending

A Double-spending attack is a type of attack where a user tries to exploit some vulnerabilities and spends the same cryptocurrency multiple times [3], [4].

2.2. A Race Attack

A race attack is a double-spending attack where someone attempts to spend the same cryptocurrency twice by sending two conflicting transactions quickly. The malicious actor sends one transaction for a service or a good and another transaction that sends the same cryptocurrency to himself. Suppose the second transaction gets mined into a block before the first one.

In that case, it can appear legitimate, causing financial loss to the seller who provided the service in anticipation of the cryptocurrency payment [5].

2.3. Finney Attack

Finney attack is a type of attack where a miner uses its mining power to execute a double-spending attack. It occurs by exploiting the vulnerability that the payments aren't yet added to the blockchain nor broadcasted to the network.

In this case, this vulnerability permits executing a double spending attack and spending the same cryptocurrency multiple times in conflicting transactions for receiving goods or services without paying a seller who expected to receive the payment [4].

2.4. Alternative History Attack

In this kind of attack, a user exploits the vulnerability of potentially controlling over 50% of the network's mining power to manipulate the blockchain's history. In this case, the miner can create a new version of the blockchain that contradicts the existing one [5].

2.5. Majority or 51% Attack

A type of attack where a user or group of users control more than 50% of the mining power and use it to manipulate the Blockchain [4], [6].

2.6. Marketplace Trader Attack

This is a refund attack that relies on social engineering techniques and the customer's trust in the reputed merchant. By exploiting the Payment Protocol and manipulating the customer's perception of the transaction, the rogue trader deceives the customer and the trusted merchant, successfully cancels the fraudulent orders, and receives a refund from the reputed merchant [7].

2.7. Silkroad Trader Attack

In such attacks, the customer exploits a vulnerability in the payment protocol by manipulating the refund address within the Payment message. This manipulation causes the refunded cryptocurrency to be sent to an illicit trader's payment address.

Subsequently, the forecited vulnerability permits the customer to deny involvement and claim that the merchant forged the message [7].

2.8. Block Withholding Attack

A type of attack where a miner intentionally does not broadcast a valid block they have mined to gain an advantage over other miners [8].

2.9. Nothing at Stake Attack

A type of attack where validators in a Proof of Stake-based blockchain can create multiple chains without incurring any cost or risk. Indeed, the consensus mechanism Proof of Stake (PoS) makes Blockchains vulnerable to such attacks [9].

2.10. Bribery Attack

A type of attack where a user pays miners to execute a majority attack and manipulate the blockchain for a short time in his favor [10].

2.11. Selfish Mining

Selfish mining is a strategy attackers employ in Blockchain systems to gain unfair advantages and maximize their rewards at the expense of honest miners. For example, the attacker can begin with Private Block Mining and then Forking a Private Chain and Mining on the Private Chain. These actions permit him to Deny Rewards to Honest Miners after Revealing Private Blocks [10].

2.12. Fork After Withholding (FAW)

A type of attack where a miner withholds a valid Proof of Work block until both of their mining pools can simultaneously propagate a valid block. This approach aims to ensure that the miner receives a reward, regardless of which block is ultimately accepted in the main chain [11].

2.13. Balance Attack

It involves producing transactions, targeting merchant subgroups, delaying messages, and manipulating the DAG tree to deceive the merchant. This attack highlights the vulnerability of PoW-based Blockchains to block manipulation and double-spending [10].

2.14. DAO Attack

DAO attack targets smart contract level. It exploits a Decentralized Autonomous Organization (DAO) vulnerability to steal funds [10].

2.15. Cryptocurrency Lost in the Transfer

A bug causing a user to lose his cryptocurrencies during a transfer due to a technical issue/error in the transaction process or the smart contract code. For example, if a user transfers a cryptocurrency to an orphaned address that doesn't have any owner or contract, the funds sent to that address would be effectively lost and inaccessible [12].

2.16. Bugs in Access Control

Bugs in access control occur when a developer forgets to apply a required modifier to a function, inadvertently exposing sensitive functionality to unauthorized users. These bugs can lead to potential security vulnerabilities and allow hackers to access and manipulate critical/sensitive parts of the contract that should have been restricted [12].

2.17. Malicious Contracts

Malicious Contracts occur when a contract calls another contract before completing its own execution, allowing the called contract to execute arbitrary code and potentially manipulate the state of the calling contract. For example, an attacker can exploit Ganache, a local Blockchain network, and a malicious smart contract by using the call function multiple times without appropriate gas limitations.

The execution continues until the user loses all their funds or reaches the maximum call stack depth. The exploited vulnerability is that once a transaction is initiated, it cannot be interrupted or modified. If an exception occurs during contract execution, the transaction is typically reverted, and any changes made to the contract state are undone [13].

2.18. Short Address Attack

When parameters are passed to a smart contract, the Ethereum Virtual Machine (EVM) encodes them according to a specific length. Suppose the provided parameters are shorter than the expected length. In that case, the EVM automatically pads zeros to the end of the encoded parameters to match the expected length.

This behavior is intended to maintain consistency and ensure that the encoded parameters are of the correct size. However, suppose a third-party application does not validate inputs and assumes that the provided parameters are of the correct length. In that case, it can be vulnerable to the attack mentioned above. Indeed, an attacker could intentionally provide shorter parameters and rely on the EVM's padding mechanism to manipulate the behavior of the smart contract [14], [15].

2.19. Cryptojacking

A type of malware permitting a hacker to use a victim's computer to mine cryptocurrency without his knowledge or consent [16].

2.20. Phishing

This act involves deceiving individuals into revealing their private keys or login credentials, intending to gain unauthorized access to their funds or sensitive information [17].

2.21. Brute Force Attack

A hacker uses a trial-and-error method to guess a user's password or other security credentials.

2.22. A Dictionary Attack

A dictionary attack involves using a list of common passwords or phrases transformed into hashed values. When a hashed value matches the password's hash, the attacker has effectively discovered and guessed the original password [17].

2.23. Vulnerable Signatures

The effectiveness of digital signatures is continuously improving, but malicious individuals have found vulnerabilities to exploit. These attackers are able to use users' private keys and sign documents and messages. Additionally, they can manipulate the content presented to the signer, inadvertently causing them to sign something different from their original intention [17].

2.24. Flawed Key Generation

During a code update, discovered vulnerabilities in the key generation process of a Blockchain-based platform could be exploited by attackers. The mistake is made during the code update, generating weak and predictable random inputs for creating public user keys. As a result, the attackers gain unauthorized access to the private keys provided by the platform. This breach compromises the security of the affected users' accounts and potentially exposes their associated Blockchain transactions to unauthorized access [12].

2.25. Attacks on Cold Wallets

A hacker exploits their knowledge of the exact timing of

a transaction or a bug to gain unauthorized access to sensitive information associated with a hardware wallet (cold wallet) or to transfer illegitimate funds into a hardware wallet [12].

2.26. Parity Multi-Sig Wallet Attack

The related code vulnerability allows an attacker to exploit the wallet and take control of millions worth of cryptocurrencies. The threat exploits a coding error (lack of a function modifier, in which the default value is public). This error allows the attacker to become the wallet owner without needing the majority of the owners' signatures [18].

2.27. Wallet Theft

During this attack, multiple techniques are utilized, including mishandling the wallet, unauthorized system breaches, and exploiting software vulnerabilities. Through unauthorized means, the attacker aims to destroy or gain illicit access to the user's private key, which leads to the loss of cryptocurrencies stored in the wallet [10].

2.28. Attacks on Hot Wallets

Hot wallets are digital wallets connected to the internet and are, therefore, more susceptible to attacks. These attacks include gaining unauthorized access to sensitive information and stealing crypto assets/funds [12].

2.29. Distributed Denial of Service (DDoS)

Engaging in DDoS attacks can be relatively low-cost but highly disruptive. Malicious miners can utilize a distributed Botnet to carry out DDoS attacks on their competitors, resulting in the expulsion of these competing miners from the network and an increase in the effective hashrate of the malicious miners. The adversary further disrupts legitimate user access by exhausting network resources [10].

2.30. Transaction Malleability Attacks

Transaction malleability attacks involve an attacker manipulating transaction IDs before they are validated on the Blockchain network. As a result, the user unknowingly pays double the intended amount, as the attacker can modify the transaction to make it appear as if it never happened. This deceptive alteration allows the attacker to debit the user twice for the same amount [17].

2.31. Timejacking

An attack on a Blockchain network where a malicious actor manipulates the network's time synchronization to trick nodes into accepting false block timestamps [17].

2.32. BGP Hijacking Attack

An attack on a Blockchain network where a malicious actor reroutes internet traffic, redirecting nodes to a false or malicious network. It can cause stealing funds [10].

2.33. Sybil Attacks

An attack on a Blockchain network where a malicious actor exploits his ability to create multiple fake identities (nodes) to control a disproportionate amount of the network's computational power, allowing them to manipulate the network [17].

2.34. Eclipse Attacks

An attack on a Blockchain network where a malicious actor isolates a node from the rest of the network, allowing him to manipulate the information received and transmitted by that node [18].

2.35. Long-Range Attacks

In this attack scenario, the integrity of the blockchain is compromised when an unethical actor creates a fork that already exists within a current block. Let's consider a scenario where a client currently has no stake in the Blockchain network but previously held a significant stake at an earlier block height.

The attacker takes advantage of the blockchain's vulnerabilities by using the private key associated with the previous block. This action allows him to generate a fork by creating a new block. Consequently, an account that lacks the current stake in the blockchain becomes vulnerable to attacks due to its lack of strong protective measures [19].

2.36. Spam Attack

An attack on a Blockchain network where a malicious actor floods the network with a large number of transactions, causing congestion and slowing down the network [19].

2.37. Targeted DDOS Attack

Targeted DDOS Attack aims to disrupt the normal functioning of the Blockchain network by flooding it with an overwhelming amount of information or requests. During such attacks, the attacker aims to introduce delays and interruptions or potentially bring the network to a complete standstill, rendering it inaccessible to legitimate users [19].

As Blockchain technology expands, users and developers must be aware of the several attacks targeting these systems. By understanding the methods and objectives of these attacks, users and developers can take steps to secure and defend their Blockchain systems against potential threats. While there is no one-size-fits-all solution to Blockchain security, knowledge, sensibilization, and awareness are important first steps toward protecting these valuable assets.

3. Materials and Methods

This section aims to analyze the layers of blockchains typically targeted by cyberattacks. Because of its general applicability in all blockchain types (permissioned, permissionless, public, and private), its focus on the blockchain system, and its ignorance of the network layer, we choose the DCEA framework.

This paper evaluates the security of the layers of the chosen framework and identifies the main cyberattacks that can target these layers by cybercriminals. In this respect, this paper presents the prominent cyberattacks on blockchain networks and systems. In addition, we provide the process used to adapt the MITRE ATT&CK framework to the blockchain context. The findings of this study will help researchers and industry professionals better understand the security risks associated with blockchain technology and develop more effective measures to mitigate or handle them.

3.1. The DCEA Framework

Blockchain technology has several layers that work together to provide a secure, decentralized, and transparent system for storing and transferring data. These layers include the Data, Consensus, Execution, and Application Layers. Each layer has its unique role and function, which contribute to the security and functionality of the Blockchain system [2].

3.1.1. Data Layer

This layer permits storing and managing data on the blockchain. It includes the data structure and protocols for storing and accessing data, such as the format for blocks and transactions.

3.1.2. Consensus Layer

This layer is accountable for ensuring that all Blockchain nodes agree on the state of the blockchain. It includes the algorithms and protocols that allow nodes to reach a consensus on the order and validity of transactions.

3.1.3. Execution Layer

This layer executes smart contracts and other decentralized applications (DApps) on the blockchain. It includes the virtual machine and programming languages permitting developers to create and deploy applications on the blockchain.

3.1.4. Application Layer

Application Layer is responsible for the user-facing applications that interact with the blockchain. It includes the user interface, decentralized applications (DApps), and APIs that allow users to access and interact with the blockchain, such as wallets, exchanges, and other applications. Figure 1 summarizes the scopes of the DCEA layers.

To sum up, the layers of a Blockchain system work together to create a decentralized system that is secure, transparent, and reliable. Each layer of the DCEA framework plays a vital role in the security and functionality of the blockchain. Understanding the different layers of a Blockchain system permits individuals and organizations to make informed decisions about the usage and interaction with this powerful technology.

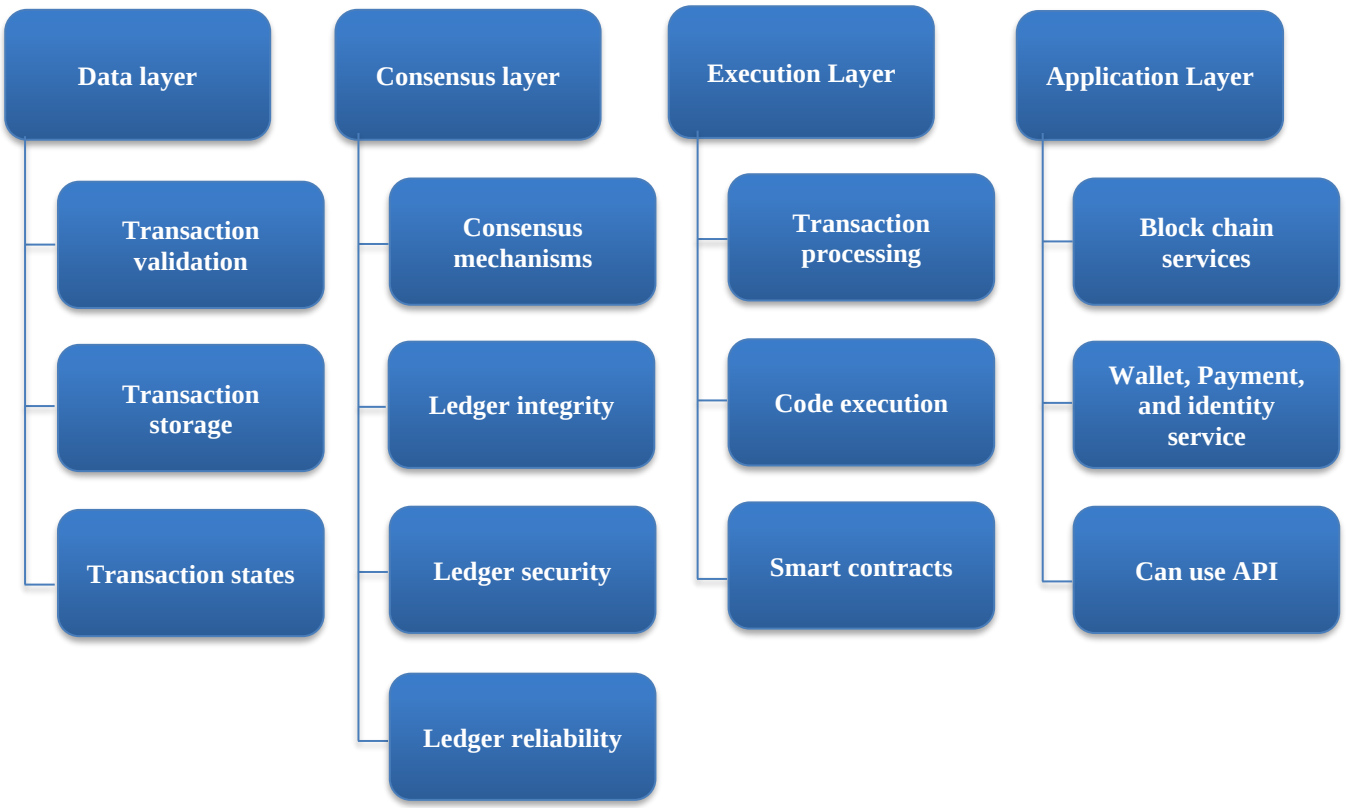

Fig. 1 DCEA framework [22]

Table 1. Major cyberattacks targeting blockchain networks and systems

Attack	Reference	Its target
Double-spending attack	[12], [19]	Consensus protocol
Race attack	[12]	Consensus protocol
Finney attack	[12], [19]	Consensus protocol
Alternative history attack	[12]	Consensus protocol
51% or Majority attack	[12], [20]	Consensus protocol
Balanced attack	[21]	Consensus protocol
Selfish mining	[12], [19]	Consensus protocol
Fork after withholding (FAW)	[12], [19]	Consensus protocol
Marketplace Trader attack	[10]	Payment Protocol
Silkroad Trader Attack	[10]	Payment Protocol
Block withholding attack	[19]	Block validation
Nothing at stack attack	[19]	Block validation
Bribery attack	[19]	Block validation
DAO attack	[19]	Smart contracts
Cryptocurrency lost in the transfer	[11], [12]	Smart contracts
Bugs in access control	[12]	Smart contracts
Malicious Contracts	[4], [13]	Smart contracts
Short address attack	[12]	Smart contracts and data structure
Cryptojacking	[16]	Wallet
Phishing	[11], [18]	Wallet
Brute force attack	[19]	Wallet
Dictionary attacks	[12]	Wallet
Vulnerable signatures	[12]	Wallet
Flawed key generation	[12]	Wallet
Attacks on cold wallets	[12]	Wallet
Parity multi-sig wallet attack	[18]	Wallet
Wallet theft	[16]	Wallet
Attacks on hot wallets	[12]	Wallet
Distributed denial of service (DDoS)	[12], [19]	network
Transaction malleability attacks	[19]	Network and data format
Timejacking	[12], [19]	network
BGP Hijacking attack	[12], [19]	network
Sybil attacks	[12], [19]	network
Eclipse attacks	[12], [19]	network
Long-range attacks	[12], [19]	network
Spam attack	[19]	Network
Targeted DDOS Attack	[12], [19]	network

3.2. The Targets of the Surveyed Attacks Related to Blockchain Networks and Systems

Blockchain networks and systems are vulnerable to many attacks. The literature review reveals and indicates the presence of more than 37 attacks targeting Blockchain networks and systems. The targets of these attacks are presented as follows in Table 1:The identified cyberattacks could lead to data breaches. Consequently, implementing security practices to handle and manage these attacks is important.

3.3. Process of Adapting the MITRE ATT&CK Framework to Blockchain Security

Adapting the MITRE ATT&CK Framework to the context of blockchain security involves tailoring the framework's tactics, techniques, and procedures to address the unique challenges and threats blockchain systems face. Here is a step-by-step process that helped us understand how to do this:

- Understand Blockchain Technology: Before adapting and applying the MITRE ATT&CK Framework to blockchain technology, we gained a solid understanding of this emerging technology. This action includes the basics of decentralized ledgers, consensus mechanisms, smart contracts, public and private keys, and other fundamental concepts.
- Identify Blockchain Threats: We identified the specific threats and attack vectors relevant to blockchain systems. These could include 51% attacks, smart contract vulnerabilities, Eclipse attacks, and Sybil attacks. Understanding these threats is needed to map them to the MITRE ATT&CK Framework.
- Map Threats to Tactics: We mapped the identified blockchain threats to the right tactics in the MITRE ATT&CK Framework. For example, a "51% attack" might map to the "Persistence" tactic. In contrast, a "smart contract vulnerability" could map to the "Execution" tactic.
- Map Techniques and Procedures: For each mapped tactic, we identified the corresponding techniques that attackers might use within the context of blockchain. Then, we outline the specific procedures attackers could follow for each technique. This step requires a deep knowledge of blockchain technology and the MITRE ATT&CK Framework fields.
- Adapt Terminology and Concepts: We ensure the terminology aligns with blockchain concepts while permitting us to adapt the framework. We Modify the descriptions and terminology to adapt the actions and behaviors to the blockchain environment accurately.
- Create a Customized Matrix: We developed a customized matrix that outlines the adapted MITRE ATT&CK framework for blockchain security. This matrix maps blockchain-related threats, tactics, techniques, and procedures.
- Include Mitigations and Countermeasures: We include relevant mitigations and countermeasures for each mapped technique and procedure to help defend against the specific threat in a blockchain context. These countermeasures are tailored to address the unique vulnerabilities of blockchain systems.
- Document and Communicate: We documented and organized my framework clearly. We consider creating tables and diagrams to help convey the information effectively to readers.

Adapting the MITRE ATT&CK Framework to blockchain security requires a deep understanding of both domains and careful consideration of the unique challenges posed by blockchain technology. It is a dynamic process that should evolve as new threats and vulnerabilities emerge in the blockchain landscape.

In summary, this section presents the DCEA framework, the targets of the main cyberattacks related to blockchain networks and systems, and the method used to adapt MITRE ATT&CK to the blockchain context. This section's information allows us to achieve this work's goal of providing layered and MITRE ATT&CK views of blockchain attacks and their related recommendations. Table 1. summarizes the targets of each layer of the DCEA framework.

4. Findings and Results

As Blockchain technology grows and becomes more commonly used, the risk of cyberattacks on these systems increases. Understanding the various attacks that can occur at each layer of a blockchain system is crucial to developing effective strategies to mitigate those risks.

In this section, this paper will examine the types of cyberattacks that can occur at each layer of a blockchain system and provide layered and MITRE ATT&CK perspectives to mitigate them using well-presented recommendations.

4.1. DCEA Layers Targeted by the Cyberattacks

The payment protocol targeted by the refund attacks is modeled in Figure 2. In this direction, it touches the wallet app and the transactions. To conclude, refund attacks target the application, execution, and data layers.The attacks concerning the Block validation target the Data and Consensus layers. The attacks related to smart contracts target the Execution layer.

The attacks targeting data structure and data format are related to the Data layer. The wallet could be a service of the application layer. Thus, the related attacks target the application layer.

Finally, network attacks are out of the scope of this paper. Figure 3 summarizes these results.

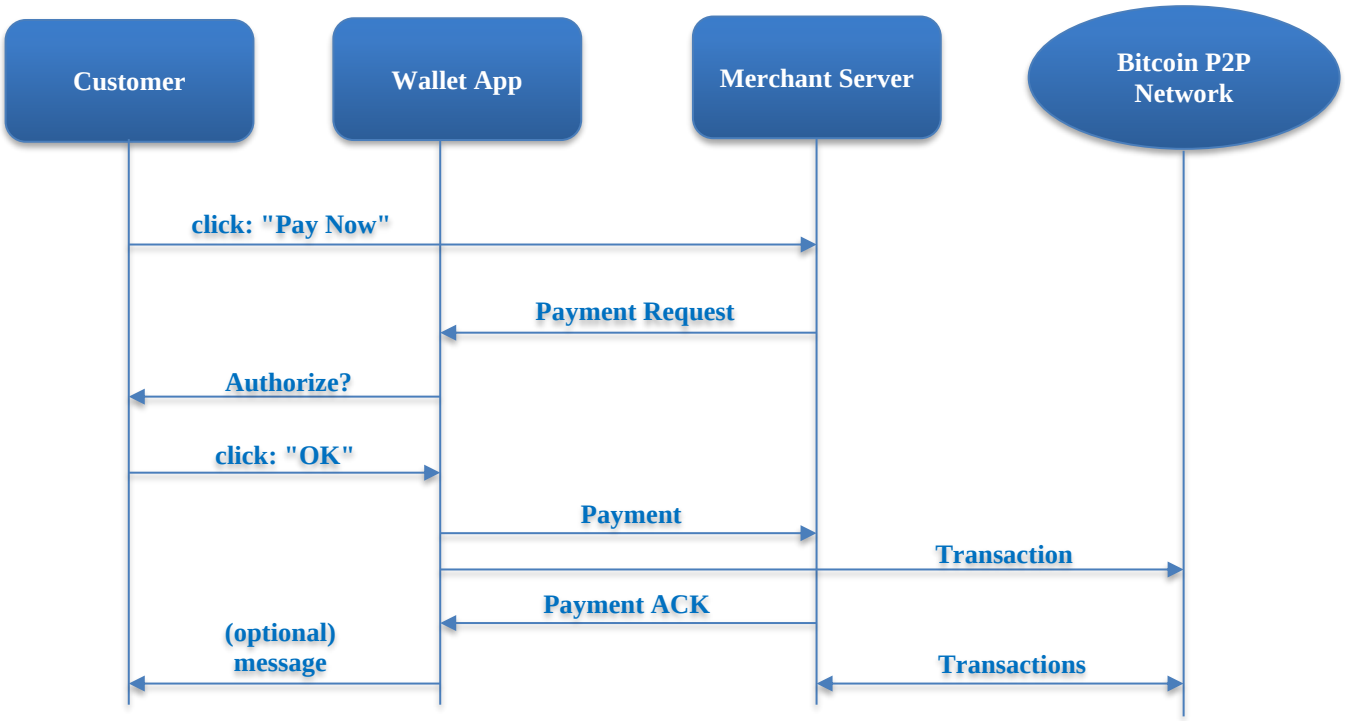

Fig. 2 The sequence diagram of the payment protocol

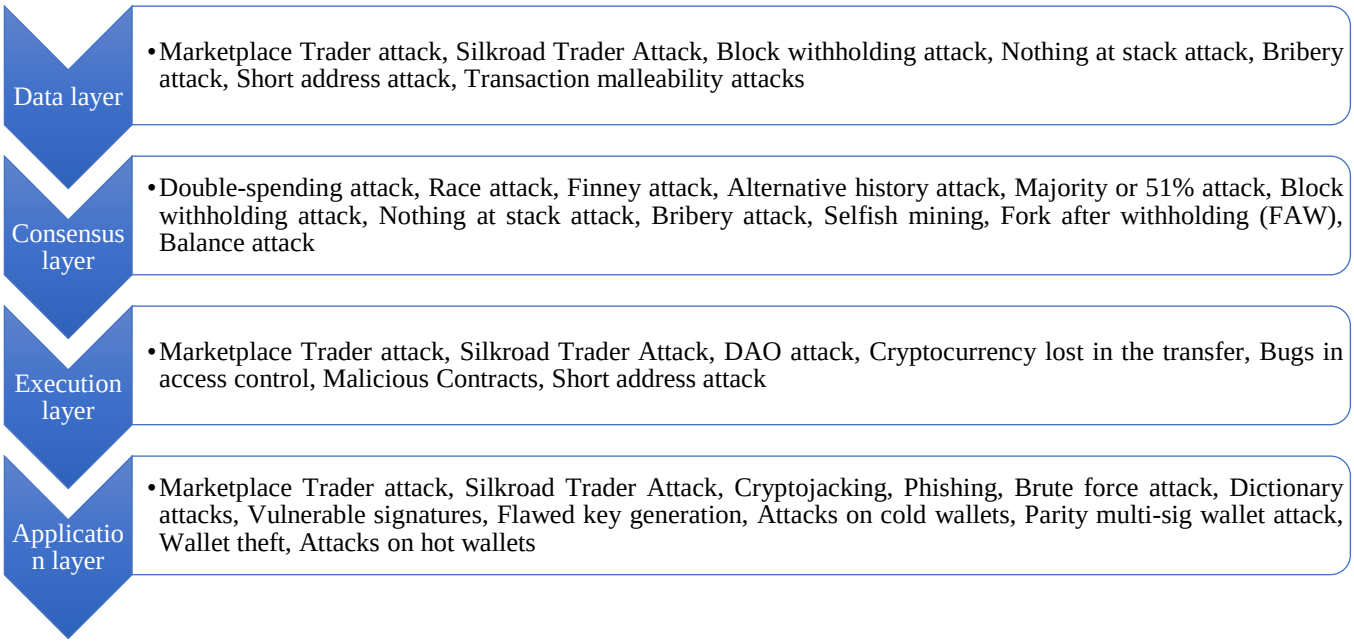

Fig. 3 Cyberattacks per DCEA layer

4.2. Recommendations

As Blockchain technology evolves and gains prominence in the digital world, so do its associated risks. Cyberattacks targeting the blockchain have become more sophisticated and frequent, with attackers exploiting vulnerabilities in Blockchain networks and systems to steal sensitive/private information or gain unauthorized access to digital assets. It is, therefore, essential to have appropriate mitigation approaches and safeguards in place to protect and defend against such risks. This subsection surveys and completes recommendations for reducing the impacts and severities of cyberattacks targeting Blockchain networks and systems. The proposed recommendations are enumerated and explained in Table 2.

Table 2. Recommendations to mitigate cyberattacks targeting blockchain systems

Attack	Related Layers	Recommendations
Double-spending attack	Consensus Layer	Use a consensus algorithm that prevents double-spending, such as Proof of Stake.
Race attack	Consensus Layer	Wait for sufficient confirmations before considering a transaction as finalized to minimize the risk of such attacks [4].
Finney attack	Consensus Layer	Use a confirmation time that prevents attackers from executing a Finney attack.
Alternative history attack	Consensus Layer	Use a consensus algorithm that makes it difficult to create alternative histories, such as Proof of Stake.
Majority, or 51% attack	Consensus Layer	Ensure no single entity controls over 50% of the network's mining power. Use a robust consensus mechanism, such as Proof of Stake.
Balanced attack	Consensus Layer	This paper recommends the following actions to mitigate such risk: Evaluate alternative consensus algorithms such as PoS or BFT consensus mechanisms class. Strengthen transaction confirmation mechanisms to make transactions more secure. Enhance block validation processes to detect suspicious or malicious behavior. Perform regular security audits of the Blockchain network. Promote education and awareness among Blockchain participants.
Selfish mining	Consensus Layer	Blockchain protocols may implement countermeasures such as adjusting block propagation protocols, increasing block confirmation requirements, or adopting consensus algorithms less susceptible to selfish mining strategies. Maintaining the integrity and security of blockchain systems in the face of sophisticated attacks like selfish mining is an ongoing challenge.
Fork after withholding (FAW)	Consensus Layer	Use a consensus protocol that detects and rejects FAW attacks if such protocol exists, or develop a new one with the forecited properties.
Marketplace Trader attack	Data, Execution, & Application Layers	Regarding accepting refund addresses over email, sharing sensitive information like refund addresses through email is generally not advisable due to security risks. Phishing attacks can exploit email communication to deceive users and gain unauthorized access to personal information. It's essential to be cautious and follow best practices to protect yourself from phishing attempts [7].
Silkroad Trader Attack	Data, Execution, & Application Layers	To mitigate such risks, merchants and payment processors must implement additional security measures, such as thorough verification processes and fraud detection mechanisms [7].
Block withholding attack	Data & Consensus Layers	A mining pool that discourages block-withholding attacks should be used to detect mechanisms and implement a protocol that penalizes miners who withhold blocks [8].
Nothing at stack attack	Data & Consensus Layers	Use a consensus algorithm that incentivizes validators to act in the network's best interest. Slashing is a punishment mechanism that can also protect against this attack [9].
Bribery attack	Data & Consensus Layers	Implement a secure consensus algorithm to ensure that miners or validators are not vulnerable to bribery.
DAO attack	Execution Layer	Make sure that smart contracts are audited and tested for vulnerabilities before deployment.
Cryptocurrency lost in the transfer	Execution Layer	Double-check transaction details and use reputable wallets and exchanges before sending cryptocurrencies. It's worth mentioning that there have been cases where individuals have lost access to their own Ethereum addresses due to losing their private keys or encountering technical issues. In those cases, recovery options might be available through backups, key management solutions, or wallet providers, depending on the specific circumstances. However, the funds sent to it are effectively lost if an address is truly orphaned with no owner or contract.
Bugs in access control	Execution Layer	This paper recommends reviewing and testing contracts, following best practices and guidelines, using automated testing tools and security audits, Employing formal verification techniques, and finally, Staying updated with security updates.

Malicious Contracts	Execution Layer	Follow secure coding practices and perform rigorous testing/auditing of smart contracts.
Short address attack	Data & Execution Layers	Third-party applications must perform thorough input validation and ensure that parameters are of the expected length. By validating inputs before interacting with a smart contract, applications can safeguard against potential attacks that exploit the EVM's padding feature and maintain the intended behavior of the contract.
Cryptojacking	Application layer	Use reputable protection tools such as No Coin and minerBlock. Don't click on suspect links or download unidentified software [16].
Phishing	Application layer	Be aware of unsolicited emails and always verify the sender's authenticity before entering sensitive information. Attend awareness sessions on social engineering attacks.
Brute force Attack	Application layer	Use strong passwords and multi-factor authentication.
Dictionary Attacks	Application layer	Use a unique and complex password that attackers cannot easily guess.
Vulnerable Signatures	Application layer	Use a secure and robust digital signature mechanism, such as TESLA, and ensure that keys are properly generated and managed. [22]
Flawed key Generation	Application layer	Security measures include implementing strong security practices during code updates and key generation, conducting regular security audits, performing thorough testing, and utilizing reliable random number generation techniques. By prioritizing security and adhering to best practices, Blockchain systems can minimize the risk of similar attacks, ensuring the integrity and confidentiality of user keys and safeguarding valuable assets.
Attacks on cold wallets	Application layer	Keep cold wallets in a safe and secure location and regularly update the software and firmware.
Parity multi-sig wallet attack	Application layer	Conduct thorough audits and vulnerability testing on the codes before deployment, primarily focusing on function modifiers.
Wallet theft	Application layer	Use reputable wallets and exchanges with robust security measures like multi-factor authentication.
Attacks on hot wallets	Application layer	Use hot wallets only for small amounts of cryptocurrency and avoid keeping large amounts in them.
Distributed denial of service (DDoS)	Out of scope (Network attack)	Use a protocol that mitigates DDoS attacks, such as rate limiting or IP filtering. Fine-tune the settings and regularly update the filters to adapt to evolving threats.
Transaction malleability attacks	Data Layer	Wait for sufficient confirmations before considering a transaction valid. Monitor transaction history for suspicious or duplicate transactions. Use multi-signature wallets that require multiple authorizations. Verify the recipient's public key or address before initiating a transaction. Follow security best practices like strong passwords and two-factor authentication. Consider using Blockchain auditing tools to detect anomalies. Stay informed, educated, and sensitized about Blockchain security.
Timejacking	Out of scope (Network attack)	Use a protocol that mitigates timejacking attacks, such as NTP (Network Time Protocol) synchronization [10].
BGP Hijacking Attack	Out of scope (Network attack)	Use BGP security measures like route filtering to prevent BGP hijacking attacks.
Sybil attacks	Out of scope (Network attack)	Implement mechanisms for unique node identification or limit control of nodes by a single entity.
Eclipse Attacks	Out of scope (Network attack)	Maintain diverse connections to other nodes and verify their authenticity.
Long-range Attacks	Out of scope (Network attack)	One possible countermeasure to mitigate such attacks is using checkpointing mechanisms. They can be implemented to verify the finality of blocks, ensuring that a recently changed fork, which did not exist in previous blocks, is not accepted [19].
Spam attack	Out of scope (Network attack)	Implement rate limiting or transaction fees to limit the number of transactions that can be added to the blockchain. The "SAGA BC" algorithm is also a preventive option [19], [23].
Targeted DDOS Attack	Out of scope (Network attack)	Use rate limiting to control the volume of incoming traffic, traffic filtering to identify and block malicious requests, deploying distributed infrastructure to distribute the load across multiple nodes, and a robust incident response plan for continuous monitoring and timely response to suspicious traffic patterns.

Table 3. Mapping of blockchain-specific tactics and techniques based on real-world threat scenario

Tactic	Technique	Procedures	Mitigations and Countermeasures
Initial Access	Blockchain Node Compromise	1. Exploit node software vulnerabilities.	- Regularly update and patch blockchain node software.
		2. Gain unauthorized access to the blockchain node.	- Implement strong access controls for node access. This paper can inspire you [24].
Execution	Smart Contract Vulnerabilities	1. Identify smart contracts with vulnerabilities.	- Follow secure coding practices for smart contracts.
		2. Exploit vulnerable smart contract code.	- Audit and review smart contract code for flaws. - Implement "ContractGuard" for detecting intrusions [15].
Persistence	Fifty-one percent Attack	1. Control over 51% of the blockchain's computational power.	- Implement consensus mechanisms with high resistance. - Think intrusion detection by design as proposed by this paper [25].
		2. Reorganize the blockchain to confirm malicious actions.	- Monitor the network for unusual computational power.
Defense Evasion	Sybil Attack	1. Create multiple fake identities (nodes).	- Implement identity verification mechanisms and prevention algorithms like the one described in this paper [26].
		2. Use Sybil nodes to control network decisions.	- Monitor for sudden increases in node count.
Credential Access	Eclipse Attack	1. Surround the target's node with malicious nodes.	- Implement a solution to detect Eclipse attacks like the one described in this paper [27]. - Maintain a diverse set of node connections.
		2. Control network communication around the target.	- Implement network-level encryption and security.
Discovery	Blockchain Analytics Deanonymization	1. Correlate transaction data to reveal identities.	- Use privacy-improving techniques like CoinJoin [28].
		2. Link addresses to real-world identities.	- Educate users on privacy best practices.
Lateral Movement	Consensus Mechanism Exploitation	1. Manipulate consensus protocol to control the Blockchain network.	- Implement consensus mechanisms with strong security as needed by the blockchain design.
Impact	Double Spending Attack	1. Spend the same cryptocurrency more than once.	- Implement mechanisms to prevent double-spending [29].
		2. Exploit the blockchain's delayed confirmation.	- Monitor for unusual transaction patterns.
		3. Disrupt the transaction confirmation process.	- Use confirmations before considering transactions.

4.3. Mapping of Blockchain-Specific Tactics and Techniques based on Real-World Threat Scenarios

The synergy between tactics and techniques becomes dominant in the ever-evolving cybersecurity landscape. Table 3. encapsulates a dynamic interaction between blockchain security and the MITRE ATT&CK framework. As blockchain technology gains momentum, its vulnerabilities need a tailored approach. Table 3 elucidates the tactics, techniques, and procedures that come into play when applying the MITRE ATT&CK framework [1] to fortify blockchain security. This table's synthesis of blockchain context and the MITRE ATT&CK framework synergy underscores the critical phase where innovative technology meets advanced threat analysis. Each cell within the table explains the dynamic facets of cyber threats and defense strategies. This comprehensive perspective equips us to decrypt the nuances of blockchain-related attacks and strengthen security through strategic mitigations.

Table 4. Case study: Real-World Attack Scenarios, Tactics, Techniques, and Mitigations

Attack Vector	Tactics	Techniques	Procedure	Mitigations
Exploiting vulnerabilities in the exchange's blockchain nodes.	Initial Access	Blockchain Node Compromise	Exploiting node software vulnerabilities or gaining unauthorized access to blockchain nodes.	Regularly update and patch blockchain node software and implement strong access controls.
Exploiting vulnerabilities in the smart contracts of the exchange.	Execution	Smart Contract Vulnerabilities	Identifying vulnerable smart contracts and exploiting their code.	Follow secure coding practices, audit, review smart contract code for flaws, and implement smart contract codes to detect intrusions.
Gaining control over 51% of the computational power to manipulate transactions.	Persistence	Fifty-one percent Attack	Gaining control over computational power and reorganizing the blockchain.	Implement high-resistance consensus mechanisms, monitor for unusual computational power, and think of intrusion detection by design.
Creating fake identities (nodes) to control network decisions.	Defense Evasion	Sybil Attack	Creating fake nodes and using them to control network decisions.	Implement identity verification mechanisms and prevention algorithms. Monitor for sudden increases in node count.
Surrounding the exchange's nodes with malicious nodes to control communication.	Credential Access	Eclipse Attack	Surrounding nodes with malicious nodes and controlling network communication.	Maintain diverse node connections and implement network-level encryption and security.
Correlating transaction data to reveal user identities.	Discovery	Blockchain Analytics, Deanonymization	Correlating data, linking addresses to identities.	Use privacy-improving techniques and educate users on privacy best practices.
Manipulating consensus protocols to control the network and move laterally.	Lateral Movement	Consensus Mechanism Exploitation	Manipulating consensus to control the network.	Implement consensus mechanisms with strong security as needed by the blockchain design.
Spending the same cryptocurrency multiple times and causing financial losses.	Impact	Double Spending Attack	Spending, exploiting delays, disrupting confirmation.	Implement mechanisms to prevent double spending, monitor for unusual transaction patterns, and use confirmations before considering transactions.

This table is a navigational beacon in fortifying blockchain security while we navigate the complex digital landscape. Adapting the MITRE ATT&CK Framework to blockchain security enhances our ability to address blockchain-related threats. The mapping of tactics and techniques bridges the gap between cybersecurity and blockchain technology, offering a comprehensive approach to safeguarding these innovative systems in an ever-evolving threat landscape. By aligning these two domains, we pave the way for more resilient and secure blockchain implementations.

4.4. Case study to illustrate how using our MITRE ATT&CK framework and Real-World Scenario: A Cryptocurrency Exchange Hack

In this scenario, a cryptocurrency exchange experiences a security breach that leads to unauthorized access and theft of users' digital assets. Through Table 4, let's analyze how the MITRE ATT&CK Framework applied to Blockchain technologies helps in identifying potential attack vectors, tactics, and techniques specific to blockchain systems based on real-world scenarios:

In this real-world scenario, our new MITRE ATT&CK framework enables security professionals to analyze the various tactics and techniques that adversaries could use to compromise a cryptocurrency exchange. By mapping the attack vectors to relevant tactics and techniques, the exchange can develop targeted mitigations and countermeasures to prevent, detect, and respond to potential attacks. This approach enhances the exchange's overall cybersecurity posture and protects its users' digital assets.

Finally, Blockchain technology is revolutionizing many industries. Consequently, its security risks must be handled

correctly by mitigating or eliminating them. Indeed, they can't be ignored. Furthermore, cyberattacks targeting the blockchain can have significant impacts, such as loss of funds or unauthorized access to sensitive information, which can negatively impact the affected parties. The suggested recommendations can help minimize the risks' severities and impact associated with the current attacks targeting Blockchain systems. Indeed, by implementing these recommendations, organizations can effectively handle the risks associated with cyberattacks targeting the blockchain and build a more secure and trustworthy digital ecosystem.

In brief, cyberattacks on blockchain networks and systems are a significant risk. It is essential to understand the methods, objectives, targets, and affected layers related to cyberattacks that can occur at each layer of the blockchain. By implementing the recommendations suggested in this section, blockchain networks and systems can be more secure and better equipped to handle potential attacks, ensuring the security and reliability of the system.

5. Conclusion

In conclusion, cyberattacks on blockchain networks and systems are a significant risk, and it is essential to understand the methods, objectives, targets, and layers of cyberattacks that can occur at each blockchain layer. By implementing the proposed recommendations, blockchain networks and systems, especially those applied to the cryptocurrency context, can be more secure, robust, and ready to better manage possible attacks, ensuring the integrity and trustworthiness of the system. Indeed, while there is no guaranteed method to eliminate all risks of attacks on Blockchains, the recommendations can help mitigate the risks and vulnerabilities.

However, it is essential to understand the several attacks that can target blockchain systems and take appropriate actions to mitigate their impact. By implementing robust security measures and safeguards and following best practices, especially those proposed by our MITRE ATT&CK framework, users and developers can cooperate to ensure the safety and security of their blockchain systems. Ultimately, all participants in the Blockchain ecosystem must work together to prevent attacks and maintain the system's integrity, especially by following best practices related to social engineering attacks. Finally, future works include using the knowledge developed in this paper to create cyber defense tools or analyze hacking tools and methodologies suitable to blockchain technology needs.

References

[1] ATT&CK Matrix for Enterprise, MITRE ATT&CK, 2023. [Online]. Available: https://attack.mitre.org/

[2] Badr Bellaj et al., "DCEA : A Reference Model for Distributed Ledger Technologies," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, pp. 1-2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Usman W. Chohan, "The Double Spending Problem and Cryptocurrencies," SSRN Electronic Journal, pp. 1-11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shubhani Aggarwal, and Neeraj Kumar, "Attacks on Blockchain," Advances in Computers, vol. 121, pp. 399-410, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xintong Ling et al., "Practical Modeling and Analysis of Blockchain Radio Access Network," IEEE Transactions on Communications, vol. 69, no. 2, pp. 1021-1037, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Nidhee Rathod, and Dilip Motwani, "Security Threats on Blockchain and its Countermeasures," International Research Journal of Engineering and Technology, vol. 5, no. 11, pp. 1636-1642, 2018. [Google Scholar] [Publisher Link]

[7] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao, "Refund Attacks on Bitcoin's Payment Protocol," International Conference on Financial Cryptography and Data Security, 20th International Conference, FC 2016, Christ Church, Barbados, pp. 581-599, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] Suhyeon Lee, and Seungjoo Kim, "Countering Block Withholding Attack Efficiently," IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, pp. 330-335, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Leonard Lys et al., "Defending Against the Nothing-At-Stake Problem in Multi-Threaded Blockchains," Arxiv, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Alireza Hedayati, and Hourieh Hosseini, "A Survey on Blockchain: Challenges, Attacks, Security, and Privacy," International Journal of Smart Electrical Engineering, vol. 10, no. 3, pp. 141-168, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Lukas Konig et al., "The Risks of the Blockchain a Review on Current Vulnerabilities and Attacks," Journal of Internet Services and Information Security, vol. 10, no. 3, pp. 110-127, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology, Apriorit, 2021. [Online]. Available: https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors

[13] Joanna Moubarak, Eric Filiol, and Maroun Chamoun, "On Blockchain Security and Relevant Attacks," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sarwar Sayeed, Hector Marco-Gisbert, and Tom Caira, "Smart Contract: Attacks and Protections," IEEE Access, vol. 8, pp. 24416-24427, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Xinming Wang et al., "ContractGuard: Defend Ethereum Smart Contracts with Embedded Intrusion Detection," IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 314-328, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Charles McFarland et al., "Blockchain Threat Report," McAfee: Cryptojacking, 2018. [Google Scholar] [Publisher Link]

[17] Dahhak Hajar, Imane Hilal, and Nadia Afifi, "Blockchain Security Attacks: A Review Study," Lecture Notes in Networks and Systems, Springer, Cham, vol. 669, pp. 191-199, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] On the Parity Multi-Sig Wallet Attack, Medium, Medium, 2017. [Online]. Available: https://medium.com/blockcat/on-the-parity-multi-sig-wallet-attack-83fb5e7f4b8c

[19] A. Begum et al., "Blockchain Attacks, Analysis and a Model to Solve Double Spending Attack," International Journal of Machine Learning, vol. 10, no. 2, pp. 352-357, 2020. [Google Scholar] [Publisher Link]

[20] Sarwar Sayeed, and Hector Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack," Applied Sciences, vol. 9, no. 9, pp. 1-17, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Christopher Natoli, and Vincent Gramoli, "The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, pp. 579-590, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Meryem Cherkaoui Semmouni, Abderrahmane Nitaj, and Mostafa Belkasmi, "Bitcoin Security with Post Quantum Cryptography," Lecture Notes in Computer Science, Springer, Cham, pp. 281-288, vol. 11704, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Koichi Nakayama, Yutaka Moriyama, and Chika Oshima, "An Algorithm that Prevents SPAM Attacks Using Blockchain," International Journal of Advanced Computer Science and Applications, vol. 9, no. 7, pp. 204-208, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Aafaf Ouaddah, "A Blockchain Based Access Control Framework for the Security and Privacy of IoT with Strong Anonymity Unlinkability and Intractability Guarantees," Advances in Computers, vol. 115, pp. 211-258, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[25] Eko Arip Winanto et al., "Designing Consensus Algorithm for Collaborative Signature-Based Intrusion Detection System," Indonesian Journal of Electrical Engineering and Computer Science, vol. 22, no. 1, pp. 485-496, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Azeem ud din Siddiqi, and Zulfikar Ali, "The Sybil Attack Prevention Algorithm: Makes Blockchain Network More Secure," International Journal of Advanced Sciences and Computing, vol. 1, no. 1, pp. 18-26, 2023. [Google Scholar] [Publisher Link]

[27] Dhanasak Bhumichai, and Ryan Benton, "Detection of Ethereum Eclipse Attack Based on Hybrid Method and Dynamic Weighted Entropy," SoutheastCon 2023, Orlando, FL, USA, pp. 779-786, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Dominic Deuber, and Dominique Schröder, "CoinJoin in the Wild: An Empirical Analysis in Dash, Lecture Notes in Computer Science," Springer, Cham, vol. 12973, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Hyunjae Lee et al., "Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain," 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Hong Kong, China, pp. 1-2, 2018. [CrossRef] [Google Scholar] [Publisher Link]