Blockchain Networks Vulnerabilities: Common Exploits and Mitigation Techniques

Group Members:

Nurdiyana Athirah Binti Abdul Karim (241UC2407E)

Ahmad Adam Affnan Bin Rozainey (241UC240C7)

Karthekeyan (1211108235)

Sinehaa A/P Paramasivam (1211103116)

Course: Research Methodologies for Computer Science

Assignment 1 - Blockchain Networks Vulnerabilities: Common Exploits and Mitigation Techniques

Date of Submission: [September 10th, 2024.]

Abstract

This literature review explores the vulnerabilities within blockchain networks and evaluates the mitigation strategies proposed across four significant research papers in the field of blockchain security. The primary objective of the review is to assess common exploits across different blockchain layers and analyze the effectiveness of proposed solutions, such as formal verification methods for smart contracts and the novel Proof of Adjourn (PoAj) consensus mechanism. The review covers a range of vulnerabilities, including smart contract weaknesses, consensus protocol flaws, and potential threats from quantum computing. Key findings indicate that while the research presents valuable contributions—such as a detailed seven-layer security framework and advanced techniques for preventing reentrancy attacks—limitations persist in areas such as empirical testing, scalability, and practical real-world application. Moreover, emerging threats, including quantum computing and blockchain centralization, remain underexplored. The review concludes that while the current body of literature offers a solid foundation for addressing blockchain vulnerabilities, further research is needed to address practical implementation issues, scalability, and new attack vectors to improve blockchain security and resilience.

Contents

1 Introduction

- **Research Problem/Question:**

  Blockchain technology has caught the world's interest with the potential to enhance its transparency, decentralisation, and security, which can completely revolutionise a variety of industries. Supply chain management, finance, and healthcare could be the few of many industries involve in the phenomenon. Blockchain networks still have a lot of security vulnerabilities, which potentially make these systems less reliable even with all of their benefits. The network, data, application, contract, consensus, and other levels make up the complex blockchain architecture. Each layer has unique vulnerabilities that can be taken advantage of. The primary research question that this literature review seeks to answer is: How can blockchain systems be protected from current and future cyberattacks using enhanced structural frameworks, innovative verification methods, and innovative consensus protocols?

- **Objectives of the Review:**

  1. To study on how relevant is the current's prevention methods in safeguarding blockchain networks.

  2. To analyse on the vital differences within existing studies in relation to the development of prevention procedures that address the problem.

  3. To study the common pattern within the blockchain security vulnerabilities and attacks with consensus network interaction, protocols and smart contracts being highlighted.debates in the research area.

- **Scope of the Review:**

  This review will cover vulnerabilities across a wide dimension of blockchain architecture, with four layers as the main pillars:

  - Contract Layer: Focusing on smart contract vulnerabilities such as reentrancy attacks and consistency issues of code.

  - Consensus Layer: Addressing threats, selfish mining, and the efficacy of various consensus mechanisms, including Proof of Stake (PoS) and the novel Proof of Adjourn (PoAj).

  - Data Layer: Discussing issues of transaction versatility and how to avoid manipulation of data by implementing technique such as Segregated Witness (SegWit).

- Network Layer: Analyse the Sybil attacks and network manipulation tactics, peer-to-peer communication (P2P) and node verification methods impact.

This research will also study the blockchain threats pattern and the future prevention needed to bolster security across decentralised networks.

2 Literature Review

2.1 Overview of Selected Papers

- **Paper 1:** Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy
  - **Citation and Authors:** Mollajafari, S.; Bechkoum, K. [], 2023
  - **Research Focus:**

    This research paper provides an in-depth analysis of the security vulnerabilities and risks associated with blockchain technology, focusing on a seven-layer architecture to dissect and address these challenges comprehensively. Blockchain technology, renowned for its decentralized nature, offers significant benefits such as enhanced transparency and support for sustainability initiatives. However, these advantages come with a range of security threats that need to be meticulously addressed. The study employs a systematic literature review of 478 sources, filtering down to 291 relevant studies, to identify vulnerabilities and attacks across each of the seven layers: Application, Contract, Incentive, Consensus, Network, Data, and Physical. Each layer is examined for its specific security risks, from hot wallet theft and smart contract vulnerabilities to cryptojacking and attacks on the physical infrastructure supporting blockchain systems. The research underscores that the Contract Layer, which includes smart contracts, is particularly prone to vulnerabilities due to its reliance on code and the immutability of deployed contracts. The paper proposes a detailed taxonomy that categorizes these vulnerabilities and attacks while offering practical countermeasures and best practices to mitigate them. Key contributions include a comprehensive review of blockchain security, a detailed

taxonomy of vulnerabilities and countermeasures, and a model application for enhancing smart contract security. Future work is recommended to focus on validating countermeasures, exploring new security techniques, and addressing centralization risks through Decentralized Autonomous Organizations (DAOs) to ensure blockchain technology's robustness and sustainability. This research lays the groundwork for further exploration into blockchain security, aiming to provide a more secure and decentralized technological framework.

– **Methodology:**

The methodology for this study involves a rigorous, systematic literature review (SLR) aimed at uncovering vulnerabilities and mitigation techniques across the blockchain's seven-layer architecture. A total of 478 academic papers, technical reports, and relevant resources were collected from established research databases such as IEEE, ACM, and ScienceDirect. This wide-ranging collection was carefully curated to ensure comprehensive coverage of blockchain security, layering structures, and specific vulnerabilities. An inclusion and exclusion criterion was applied to filter down to 291 articles, ensuring that only the most relevant studies contributed to the research. The inclusion criteria focused on papers that directly address blockchain technology's security, vulnerabilities in blockchain architecture, and countermeasures for potential exploits, while the exclusion criteria eliminated studies with outdated or insufficient technical depth. The seven-layer blockchain model was used to structure the thematic analysis, which facilitated the classification of security risks at each layer—Application, Contract, Incentive, Consensus, Network, Data, and Physical.

The selected studies were thoroughly analyzed, with a focus on identifying the most common and high-impact security risks, vulnerabilities, and the mechanisms employed by attackers. A thematic analysis was employed to extract and classify data related to vulnerabilities, based on the specific layers they affect. Particular attention was given to both blockchain-specific risks, such as smart contract vulnerabilities, as well as broader cybersecurity threats, including DDoS, Sybil attacks, and DNS vulnerabilities. In addition to textual data from academic resources, real-world data from open-source repositories

such as GitHub and Etherscan were gathered to support the analysis of smart contract vulnerabilities and network-level attacks. The data from smart contract repositories provided practical examples of how certain vulnerabilities could be exploited, while thematic analysis allowed for categorization of these risks into the seven-layer architecture.

The research also involved a detailed evaluation of countermeasures, focusing on their practicality and effectiveness in mitigating identified risks. Various proposals from existing literature were systematically examined, particularly the defensive mechanisms designed to reduce centralization risks in Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms. The thematic approach was instrumental in mapping risks to specific layers and identifying recurring security themes, such as centralization in the Consensus and Incentive Layers, as well as the exploitation of smart contracts in the Contract Layer. Overall, this methodology enabled the development of a robust taxonomy of blockchain vulnerabilities, attacks, and countermeasures, laying the foundation for the proposed model application to enhance the security of smart contracts and other layers of the blockchain architecture.

– **Key Findings:**

The research uncovered several critical findings that contribute significantly to understanding blockchain security risks across the seven-layer blockchain architecture. One of the most profound discoveries was the layered structure's inherent vulnerabilities, with each layer susceptible to different types of attacks, highlighting the need for targeted countermeasures.

2.1.1 Application Layer

This layer is responsible for managing interactions between users and applications, was found to be particularly vulnerable to risks associated with centralization. Malicious actors can exploit centralized platforms, such as centralized exchanges, to manipulate transactions or perform unauthorized actions. Moreover, this layer also revealed risks related to malicious third-party applications that can inject malicious code or take advantage of vulnerabilities within decentralized applications (dApps).

2.1.2 Contract Layer

Smart contracts were identified as a major source of vulnerabilities, given their irreversible and autonomous nature once deployed. Several exploits, such as reentrancy attacks and mishandling of contract permissions, were found to be a frequent occurrence. These attacks enable malicious actors to drain funds or take over contracts due to bugs and vulnerabilities in the smart contract code. Since smart contracts operate on an immutable blockchain, any security flaws discovered after deployment cannot be easily corrected, making security auditing crucial before implementation. The study found that developers' over-reliance on manually coded rules and algorithms increased the risk of these vulnerabilities, particularly in platforms like Ethereum that rely heavily on smart contracts. This layer emerged as one of the most significant threats to blockchain security, as any compromise here directly impacts the entire blockchain ecosystem.

2.1.3 Incentive and Consensus Layers

Identified as critical areas prone to security risks, mainly due to the centralization tendencies within mining pools and the underlying weaknesses in consensus algorithms. In the Incentive Layer, the existence of large mining pools was found to lead to disproportionate reward distribution, skewing incentives and potentially making the system less secure. The research found that mining centralization can lead to vulnerabilities like bribery attacks, where attackers attempt to bribe miners to manipulate the blockchain for double-spending. On the other hand, the Consensus Layer exhibited vulnerabilities in the consensus mechanisms, particularly in Proof of Work (PoW) and Proof of Stake (PoS) systems. PoW, for instance, is vulnerable to 51 percentage of attacks when a malicious actor controls more than half of the network's mining power, allowing them to manipulate transaction records and create forked chains. PoS, while less energy-intensive, poses its risks, particularly around governance and validator collusion, where validators can form coalitions to manipulate the consensus process.

2.1.4 Network Layer

The study found this layer to be particularly susceptible to network-based attacks, including Distributed Denial of Service (DDoS) attacks, Sybil attacks, and Border Gateway Protocol (BGP) hijacking. A DDoS attack can overwhelm a blockchain network, clogging memory pools with excessive transactions, which leads to backlogs and increased fees for users. Sybil attacks, where attackers create numerous fake identities to flood the network, were found to disrupt block propagation and make consensus difficult, leading to network splits and potential double-spending attacks. Moreover, the Network Layer revealed vulnerabilities in the use of Domain Name System (DNS) services, which expose blockchain systems to centralization risks and single points of failure. Attackers can exploit weaknesses in DNS protocols to reroute blockchain traffic, leading to malicious redirection and transaction tampering.

2.1.5 Data Layer

The research highlighted the risk of transaction malleability attacks and timejacking. Transaction malleability involves altering the transaction ID (TXID) before it is confirmed on the blockchain, allowing an attacker to manipulate the transaction while still appearing valid. This type of attack can result in double-spending and undermines the trustworthiness of blockchain transactions. Timejacking, on the other hand, involves altering the timestamps of blocks, allowing attackers to manipulate the order of transactions on the blockchain and potentially cause network splits. The study found that these attacks are particularly problematic for cryptocurrencies, where transaction order and confirmation times are crucial for maintaining integrity.

2.1.6 Physical Layer

This layer's focus was primarily on hardware-related security risks, such as cold wallet theft and cryptojacking malware. Cold wallets, often consid-

ered one of the most secure means of storing private keys, were found to be vulnerable to physical theft and man-in-the-middle (MITM) attacks when connected to compromised terminals for transactions. Additionally, the research revealed that cryptojacking, where attackers secretly use the computational power of devices to mine cryptocurrencies, is becoming increasingly common, with both executable-based and browser-based methods being employed. This highlights the risks associated with integrating blockchain technologies with physical devices and the importance of securing hardware endpoints to prevent unauthorized access to sensitive assets.

Overall, the findings of this study emphasize the diverse nature of blockchain vulnerabilities and the importance of a multi-layered approach to security. The study underscores the need for rigorous auditing, secure coding practices, and the development of decentralized solutions to minimize centralization risks across layers. Additionally, while blockchain-based solutions like Ethereum Name Service (ENS) can help mitigate some of the DNS centralization risks, they also present new challenges in the form of smart contract vulnerabilities. The research concluded that while blockchain offers robust security advantages in many areas, its adoption and sustainability hinge on addressing these vulnerabilities systematically across each layer of the architecture.

- **Paper 2:** Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract
  - **Citation and Authors:** Kushwaha, S. S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.-N. [], 2022
  - **Research Focus:**

    This paper provides a thorough analysis of the Ethereum blockchain's security vulnerabilities. The primary goal is to go over real-world attacks, detection tools, security flaws in Ethereum smart contracts, and countermeasures. By taking into account different properties, comparisons between the Ethereum smart contract analysis tools are conducted. Several problems with the Ethereum blockchain-based smart contract are brought to light by the thorough depth review. The need for a detailed, structured review of Ethereum

smart contract vulnerabilities is evident due to gaps in existing surveys. This study addresses these gaps by presenting a systematic analysis of vulnerabilities, their detection methods, and best practices for prevention.

– **Methodology:**

The authors of this study implement a systematic review methodology. The process starts with formulating important research questions that focus on finding Ethereum smart contract vulnerabilities, their underlying causes and secondary causes, and the methods that may be used to detect them. In order to resolve all these concerns, 454 peer-reviewed publications were collected by the authors from five scientific databases consisting of IEEE Xplore, Springer, ACM Digital Library, Elsevier, and Google Scholar in order to conduct a more thorough and detailed literature review. The publications of the vulnerabilities of the Ethereum smart contract were screened according to the inclusion and exclusion criteria after a keyword search focused on the specific topic was dispatched. Moreover, it is noted that the authors followed systematic study methods outlined by Kitchenham and Peterson. From an initial pool of 454 research articles, 119 were selected based on exclusion and inclusion criteria. The research questions guiding the study are:

RQ1: What are the existing vulnerabilities in Ethereum Smart Contracts?

RQ2: What are the main root causes of vulnerabilities in Ethereum Smart Contracts?

RQ3: What are the sub-causes of vulnerabilities in Ethereum Smart Contracts?

RQ4: What are the detection tools for vulnerabilities in Ethereum Smart Contracts?

The amount of papers chosen by year and database was represented in the review process using bifurcation figures and selection technique, ensuring a thorough and orderly analysis of Ethereum smart contract.

– **Key Findings:**

The research highlights several critical vulnerabilities in Ethereum smart contracts, each with unique implications and preventive strategies.

SPL-V14 (Floating Pragma) reveals the risks associated with using outdated

compiler versions, which can introduce bugs if the deployed version differs from the tested one. To mitigate this, it is essential to lock the pragma version in the Solidity source code to ensure consistency between testing and deployment.

SPL-V15 (Function's Default Visibility) underscores the importance of correctly specifying function visibility in Solidity. Failure to do so can inadvertently expose functions to unauthorized access. Developers should explicitly define visibility for all functions and heed compiler warnings about missing visibility settings.

SPL-V16 (Delegate Call) discusses the security concerns related to the 'DELEGATECALL' function, which preserves the caller's context and can lead to vulnerabilities if not managed carefully. Using the 'Library' keyword for stateless library contracts can help prevent these issues.

SPL-V17 (Unprotected 'Self-Destruct') addresses the risks of the 'selfdestruct' opcode, which can be misused to destroy contracts and misappropriate funds if access controls are not stringent. It is advisable to remove 'selfdestruct' from contracts unless absolutely necessary and, if used, employ a multi-signature scheme to add an extra layer of security.

EVM-V1 (Immutable Bugs or Mistakes) highlights the challenge of immutability in Ethereum, where deployed contracts cannot be altered, posing risks if bugs are present. Marino et al. proposed standards for contract modification and termination to address this issue.

EVM-V2 (Ether Lost in Transfer) focuses on the problem of losing ether due to incorrect recipient addresses. Manual verification of addresses is crucial to prevent irreversible loss.

EBD-V1 (Timestamp Dependency) points out the vulnerability of relying on block timestamps, which can be manipulated by miners. Using block numbers instead of timestamps can mitigate this risk.

EBD-V2 (Lack of Transactional Privacy) addresses privacy concerns, as transaction details are publicly visible. Encrypting contracts or using privacy-preserving frameworks like Hawk can enhance confidentiality.

EBD-V3 (Transaction Ordering Dependency) reveals how transaction execution order can be exploited if not managed properly. Implementing pre-commit

schemes or guard conditions can ensure the correct order of transactions.

EBD-V4 (Untrustworthy Data Feeds) emphasizes the risk of relying on external data sources, which may not be trustworthy. Tools like Town Crier act as intermediaries to ensure data integrity and privacy through encryption. Each of these findings underscores the need for vigilant security practices and advanced tools to safeguard Ethereum smart contracts against potential threats.

- **Paper 3:** A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions
  - **Citation and Authors:** Dwivedi, K.; Agrawal, A.; Bhatia, A.; Tiwari, K. [], 2024
  - **Research Focus:**

    Because blockchain technology is decentralized and irreversible, it has completely changed a number of industries, including supply chain management, healthcare, and banking. Peer-to-peer networking, cryptography, and consensus techniques are all combined to produce a decentralized ledger that securely records transactions without the need for middlemen. However, blockchain networks are vulnerable to a variety of threats and weaknesses despite its promise of security and openness. The application, contract, consensus, network, and data layers—among the several layers of the blockchain architecture— often have these vulnerabilities built in (2404.18090v1). The inherent security threats associated with blockchain technology are expected to increase in tandem with its further evolution and widespread adoption. Strong mitigation measures are essential, as seen by the growing frequency of threats like the 51 percent of attack, smart contract exploits, and cross-chain vulnerabilities. Despite the increased security that blockchain technology promises, there are still several layers in the system's architecture that are open to assault. Every layer has unique vulnerabilities that malicious actors can take advantage of. It is crucial to fix these vulnerabilities in order to maintain the integrity of the blockchain as its use increases. The goal of this research is to identify and analyze typical blockchain network weaknesses and assaults, including 51 percent of attacks, smart contract vulnerabilities, and other blockchain layer

concerns. In order to protect blockchain systems, the project will also investigate mitigating techniques such strengthening consensus processes and smart contract security (2404.18090v1).

– **Methodology:**

The present study employs an approach that entails a comprehensive examination of diverse blockchain vulnerabilities, classified according to the affected layers. Vulnerabilities can be found and particular attacks linked to these vulnerabilities can be determined by methodically examining each layer of the blockchain.

Application Layer: Application-layer attacks usually take advantage of flaws in user-end apps that interface with the blockchain and zero-confirmation transactions. Attackers take advantage of insufficient transaction validation or racial circumstances (2404.18090v1).

Contract Layer: Smart contract vulnerabilities, such as reentrancy attacks and transaction origin attacks, can affect the contract layer. Self-executing smart contracts, which frequently entail large financial transactions, are especially prone to errors and unwanted inputs (2404.18090v1).

Consensus Layer: Blockchain integrity depends on consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS). These consensus systems have weaknesses that are exploited by attacks like the 51 percent of attack and selfish mining (2404.18090v1).

Network Layer: Peer-to-peer communication between nodes is made possible via the network layer, which is vulnerable to attacks such as timejacking and Sybil, in which an attacker manipulates the network or floods it with malicious nodes (2404.18090v1).

– **Key Findings:**

Based on the key vulnerabilities found in various blockchain levels, the research categorized a variety of attacks. The papers highlights the various vulnerabilities at each tier of the blockchain architecture and offers a thorough classification of blockchain attacks. It also provides attack mitigation techniques. Here is a rundown of several significant assaults and suggested countermeasures:

Race Attacks (Application Layer): Attackers race two almost simultaneous payments to take advantage of zero-confirmation transactions. As part of mitigation, transactions must be confirmed before being processed (2404.18090v1).
- Reentrancy Attacks (Contract Layer): These attacks use smart contract recursive calls that are harmful. Updating user balances prior to performing external calls and putting in place reentrancy checks are two suggested mitigating techniques (2404.18090v1).
- Sybil Attacks (Network Layer): Malicious actors create fictitious identities, or "nodes," in order to isolate targets and initiate attacks. In order to mitigate this, trustworthy node identification techniques must be put in place, and network behavior must be watched for unusual activity (2404.18090v1).
- 51 percentage Attack (Consensus Layer): Malicious miners take over the bulk of the network in this assault, giving them the ability to reverse transactions or commit double spending. Changing to different consensus techniques, such as PoS, and enhancing network decentralization are examples of mitigations (2404.18090v1). Pros:
All layers of blockchain vulnerabilities are addressed in detail by the research, which offers a clear framework for comprehending how assaults happen at each stage. - Enforcing confirmations to thwart race attacks and putting in place node reputation systems to counter Sybil attacks are just two examples of the useful and pertinent mitigation solutions that have been suggested (2404.18090v1). Cons:
- Smaller blockchain networks with insufficient decentralization may not benefit fully from some mitigation strategies, such as those addressing 51 percent assaults (2404.18090v1).
- Comprehensive code audits and formal verification are necessary to address smart contract vulnerabilities like reentrancy attacks, but they can be time- and resource-consuming (2404.18090v1).

- **Paper 4:** Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks
  - **Citation and Authors:** Sayeed, S.; Marco-Gisbert, H. [], 2020

– **Research Focus:**

Despite blockchain's promise of enhanced security, several layers within the blockchain architecture remain vulnerable to malicious exploitation. Each layer has distinct vulnerabilities that attackers can leverage, jeopardizing the integrity of blockchain systems. As blockchain adoption expands, it becomes crucial to address these vulnerabilities to maintain trust and security. This article aims to identify and analyze common blockchain network vulnerabilities, such as 51 percent of attacks and smart contract weaknesses, and assess risks at various layers of the blockchain architecture. It will also explore mitigation techniques, such as strengthening consensus mechanisms and improving smart contract security, to safeguard blockchain networks.

– **Methodology:**

This research utilizes a comprehensive review approach to classify and examine vulnerabilities in blockchain networks, focusing on different layers of the architecture.

- Reentrancy Attacks (Contract Layer): Reentrancy attacks involve malicious recursive calls in smart contracts, allowing attackers to drain funds before the contract's state is updated. Mitigation techniques include updating user balances before external calls and implementing reentrancy checks to prevent multiple withdrawals.

- Sybil Attacks (Network Layer): In a Sybil attack, adversaries create multiple fake identities or nodes to isolate targets and manipulate the network. Countermeasures include implementing reliable node identification systems and monitoring network behavior for anomalies.

- 51 percent of Attack (Consensus Layer): A 51 percent of attack occurs when malicious miners control more than half of the network's hashing power, enabling them to reverse transactions or double-spend coins. Transitioning to alternative consensus mechanisms like Proof of Stake (PoS) and enhancing network decentralization can mitigate these attacks.

– **Key Findings:**

2.1.7 Consensus Layer Vulnerabilities

- 51 percent Attack: In a 51 percent attack, miners controlling the majority of hashing power can alter the blockchain, reverse transactions, and engage in double-spending. This attack undermines the integrity of the network by allowing one party to exert excessive control. Mitigation techniques include adopting more decentralized consensus mechanisms like PoS, improving miner distribution, and incorporating penalty systems like Proof of Adjourn (PoAj).

  - Selfish Mining: Selfish mining involves miners keeping newly discovered blocks private and mining on a separate chain. When their private chain grows longer than the public one, they release it, causing honest miners to waste resources. PoAj also addresses selfish mining by applying penalties and incentivizing proper block submission.

2.1.8 Smart Contract Layer Vulnerabilities

- Reentrancy Attacks: These attacks, specific to Ethereum, occur when an attacker recursively calls a smart contract's function, allowing them to withdraw more funds than should be possible. Proper coding practices, such as updating balances before making external calls and incorporating reentrancy locks, can prevent these attacks.

  - DoS and Redirect Attacks: Attackers can exhaust gas limits or redirect contract calls to malicious or unavailable addresses, disrupting smart contract execution. Mitigating these risks involves optimizing gas usage and incorporating fallback functions to handle failed calls.

2.1.9 Network Layer Vulnerabilities

Sybil Attacks: Malicious actors flood the network with fake identities to control a disproportionate number of nodes, allowing them to isolate honest nodes and degrade network performance. Monitoring unusual behavior, employing reliable identity verification, and strengthening peer-to-peer communication can mitigate Sybil attacks.

2.1.10 Data Layer Vulnerabilities

Transaction Malleability: In this attack, an adversary alters the transaction ID before it is confirmed, allowing them to manipulate the transaction without changing its details. Segregated Witness (SegWit) has been proposed as a solution to this vulnerability by separating transaction data from signatures.

2.2 Critical Analysis of Each Paper

- **Paper 1:** Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy

  - **Strengths:**

    Robust Methodology: The paper employs a systematic literature review methodology, meticulously analyzing a comprehensive array of sources to build a seven-layer blockchain architecture framework. This approach ensures a thorough exploration of each layer's vulnerabilities and risks, supported by an extensive review of current research, which adds credibility and depth to the findings. The use of detailed categorization into seven distinct layers allows for a nuanced understanding of blockchain security risks, enhancing the granularity and applicability of the analysis.

    Originality of the Research Question: The focus on developing a seven-layer architecture for blockchain security is a novel approach. By breaking down the blockchain into distinct layers, the paper offers a structured way to analyze security threats and vulnerabilities that is more detailed than traditional single-layer models. This original perspective allows for a more comprehensive examination of the complexities involved in blockchain security, setting the paper apart from other studies that may not differentiate between various layers and their specific risks.

    Significance of the Findings: The findings of the paper are highly significant, as they not only identify and categorize a broad spectrum of vulnerabilities and attacks but also provide a taxonomy that can be used to develop targeted countermeasures. The detailed analysis of smart contracts and their

inherent vulnerabilities, in particular, highlights crucial areas where security improvements are needed. The paper's contributions are valuable for developers, researchers, and policymakers looking to enhance blockchain security and address emerging threats.

– **Weaknesses:**

Potential Biases in Source Selection: The reliance on a systematic literature review, while comprehensive, may introduce biases based on the availability and selection of sources. If certain studies or perspectives were underrepresented or omitted, the findings might not fully capture the entire landscape of blockchain security risks. Additionally, the paper's conclusions are dependent on the quality and relevance of the reviewed literature, which may vary.

Lack of Empirical Data: The study primarily relies on secondary research and theoretical frameworks, which, while detailed, may lack empirical validation. The absence of primary data or case studies means that the proposed taxonomy and findings are based on existing literature rather than real-world testing or direct observation of blockchain implementations. This limits the ability to assess the practical effectiveness of the proposed countermeasures in live environments.

Scope of Analysis: While the seven-layer model is a significant advancement, it may still oversimplify some aspects of blockchain security. For instance, the paper might not fully address the interactions and dependencies between layers, which could affect the overall security posture. Furthermore, emerging technologies and evolving attack vectors may not be fully covered, potentially limiting the paper's applicability to future developments in blockchain technology.

– **Relevance:**

The paper is highly relevant to the field of blockchain security and contributes significantly to the broader understanding of the research question. By proposing a seven-layer architecture, it provides a detailed framework for analyzing and addressing security risks in blockchain systems. This approach is valuable for advancing knowledge in the field and can serve as a foundation for future research and practical applications.

For researchers focused on blockchain technology, the paper offers a structured way to categorize and understand security threats, facilitating more targeted and effective mitigation strategies. It also highlights the importance of addressing smart contract vulnerabilities, a critical area of concern in blockchain development. The proposed taxonomy and model for smart contract security can guide developers in implementing best practices and enhance the overall robustness of blockchain systems.

In summary, the paper's strengths lie in its innovative approach and thorough methodology, while its weaknesses include potential biases and lack of empirical data. Despite these limitations, its relevance to the field is substantial, providing valuable insights and a framework for advancing blockchain security research and practice.

- **Paper 2:** Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract

  - **Strengths:**

    Robust Methodology: The paper employs formal verification methods to analyze reentrancy attacks in smart contracts, which is a rigorous and systematic approach. Formal verification is known for its ability to mathematically prove the correctness of smart contract code, making it highly reliable in identifying vulnerabilities that might be missed by conventional testing methods. This methodological strength enhances the credibility of the findings and provides a solid foundation for the proposed solutions.

    Originality of Research Question: The focus on reentrancy attacks and their prevention through formal verification is both timely and relevant. Reentrancy attacks have been a prominent issue in smart contracts, and the paper's exploration of formal verification methods to address this specific vulnerability adds valuable originality to the field. The research contributes new insights into how formal methods can be effectively applied to secure smart contracts against complex attack vectors.

    Significance of Findings: The paper's findings are significant as they address a critical vulnerability in blockchain networks. By providing formal methods

for detecting and preventing reentrancy attacks, the paper offers practical solutions that can enhance the security of smart contracts. The implications of these findings are far-reaching, potentially influencing how developers approach security in smart contract development.

- **Weaknesses:**

  Potential Methodological Limitations: While formal verification is a robust method, it may not always account for all practical scenarios, especially in real-world applications. The paper may rely on theoretical models or controlled environments, which could limit the applicability of its findings to more complex or variable real-world conditions. Additionally, formal verification can be resource-intensive and may not always be feasible for all smart contract deployments.

  Limited Scope of Analysis: The paper focuses primarily on reentrancy attacks, which, while important, is just one type of vulnerability among many in smart contracts. The narrow focus may mean that other significant vulnerabilities are not addressed or considered in the context of formal verification. This limited scope could affect the comprehensiveness of the research and its applicability to a broader range of security issues.

  Sample Size and Practical Testing: If the paper's validation of formal methods is based on a small set of smart contracts or a limited range of use cases, this could impact the generalizability of its findings. A broader range of sample contracts and real-world scenarios would strengthen the research and provide more robust evidence of the effectiveness of the proposed methods.

- **Relevance:**

  The paper is very relevant to the broader field of blockchain security and smart contract vulnerabilities. It makes a significant contribution by tackling a common and serious threat known as reentrancy attacks and suggesting formal verification methods to prevent these attacks. This is especially valuable for researchers and practitioners working to improve smart contract security and develop better tools for detecting and preventing vulnerabilities.

  The emphasis on formal verification is timely, given the increasing need for thorough methods to ensure blockchain systems are safe and reliable. By

exploring formal verification techniques, the paper helps deepen our understanding of how to protect smart contracts and improve security practices in the blockchain space. However, addressing its limitations and broadening its focus could make its findings even more impactful and widely applicable.

- **Paper 3:** A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions

  - **Strengths:**

    Detailed Analysis and Classification: The paper provides a thorough classification of blockchain vulnerabilities and attacks based on the layered architecture. This framework enhances understanding of where specific threats originate and their implications for blockchain systems.

    Mitigation Strategies: The paper offers a range of mitigation strategies for the identified vulnerabilities. For instance, it highlights recent advancements in libraries that address key reuse vulnerabilities and proposes the use of quantum-resistant cryptographic methods, like lattice-based and code-based cryptosystems, to future-proof blockchain systems against quantum attacks.

    Emerging Technologies and Solutions: The discussion on quantum computing and post-quantum cryptography provides valuable insights into how blockchain technology might evolve. It suggests both quantum-resistant algorithms and the integration of quantum computing into blockchain systems, such as through quantum blockchains, to address future security challenges.

    Practical Implications: The paper includes practical suggestions for mitigating quantum threats, such as regular key rotation, adopting multi-signature wallets, and transitioning to post-quantum cryptographic solutions. These measures offer immediate steps to enhance security in the face of evolving threats.

  - **Weaknesses:**

    Lack of Qualitative Performance Analysis: The study does not provide a qualitative assessment or in-depth performance analysis of existing countermeasures. This gap means that while the paper outlines various mitigation strategies, it does not measure their effectiveness in practical scenarios.

Emerging Vulnerabilities: The evolving nature of technology and threats means new vulnerabilities may arise that are not covered by the current mitigations. The paper acknowledges this but does not offer specific solutions for these potential future threats.

Implementation Challenges: The proposed mitigations, such as the transition to quantum-resistant cryptography or quantum blockchains, may face implementation challenges. There is a noted lack of large-scale initiatives that can accelerate the adoption and development of these advanced technologies.

– **Relevance:**

The classification framework and mitigation strategies presented in the paper offer a strategic approach to addressing blockchain security concerns, providing valuable insights for researchers and developers. By dissecting vulnerabilities at various layers of blockchain architecture, the paper equips stakeholders with a comprehensive understanding of where specific threats originate and how they impact blockchain systems. The exploration of quantum computing's implications and the proposed solutions, including post-quantum cryptographic methods and quantum blockchain technologies, is particularly pertinent as it addresses future threats and suggests ways to safeguard blockchain systems amidst evolving technology. This foresight is crucial for ensuring the longevity and security of blockchain systems as quantum computing advances.

Furthermore, the paper guides researchers in focusing their efforts on specific vulnerabilities and effective mitigation techniques, highlighting the critical need to address blockchain centralization and 51 percent of attacks. By identifying gaps in current mitigation strategies and suggesting areas for further research, the paper lays a foundation for future studies and advancements in blockchain security. Its practical recommendations, such as key management practices, quantum-resistant algorithms, and multi-signature wallets, offer actionable steps for enhancing the security of current blockchain implementations. This makes the paper highly relevant not only for immediate improvements but also for preparing blockchain systems for future challenges, thereby contributing to a more secure and resilient blockchain ecosystem.

- **Paper 4:** Proof of Adjourn (PoAj): A Novel Approach to Mitigate

– **Strengths:**

Innovative Approach: The Proof of Adjourn (PoAj) consensus protocol is a novel contribution to blockchain security. By addressing multiple critical vulnerabilities such as selfish mining, transaction delays, and various attack vectors, PoAj introduces a new methodology that is not only unique but also potentially transformative for blockchain technology.

Comprehensive Attack Coverage: The paper effectively analyzes how PoAj mitigates several significant blockchain attacks, including 51 percent of attacks, selfish mining, miner bribes, and zero and one confirmation attacks. This thorough analysis demonstrates the robustness of the proposed solution in handling a wide range of security threats.

Detailed Implementation and Evaluation: The implementation of PoAj in Python and the detailed evaluation of its effectiveness provide practical insights into the protocol's application. The implementation is presented with clear steps and verification criteria, enhancing the understanding of how PoAj operates in real-world scenarios.

Enhanced Transaction Processing: PoAj's approach to mitigating transaction confirmation delays is particularly noteworthy. By prioritizing larger transactions and reducing waiting times, PoAj addresses a significant issue in blockchain networks, potentially improving the overall efficiency and user experience.

– **Weaknesses:**

Complexity of Implementation: The two-phase verification process introduced by PoAj may add complexity to blockchain systems. Implementing such a protocol could be challenging and may require substantial changes to existing network architectures, which could impact adoption and integration.

Scalability Concerns: The paper does not extensively address how PoAj performs under high transaction volumes or in large-scale networks. Its effectiveness and efficiency in real-world scenarios with diverse and high-load conditions remain uncertain and need further exploration.

Potential Network Disruption: The penalty system for discarded blocks and malicious nodes could lead to disruptions in network operations. The impact

of these penalties on network stability and miner incentives is not thoroughly analyzed, which could have implications for the practical deployment of PoAj. Limited Scope of Evaluation: While the paper evaluates PoAj against specific attacks, it does not comprehensively address all potential vulnerabilities or limitations. The evaluation might benefit from a broader assessment of how PoAj performs in various blockchain environments and under different attack scenarios.

– **Relevance:**

The paper's exploration of the Proof of Adjourn (PoAj) consensus protocol is highly pertinent to the field of blockchain security. By addressing several critical vulnerabilities and enhancing transaction processing, PoAj provides a significant advancement in blockchain technology. Its novel approach to mitigating common attacks such as 51 percent attacks, selfish mining, and transaction confirmation delays makes it a valuable contribution to the ongoing efforts to improve blockchain consensus mechanisms. The practical implementation and detailed evaluation of PoAj offer actionable insights for both researchers and practitioners, guiding future developments in blockchain security. Furthermore, the paper sets the stage for future research, encouraging further investigation into PoAj's scalability and effectiveness across various blockchain environments. This makes the paper a crucial resource for advancing the understanding and application of secure blockchain protocols.

2.3 Comparative Analysis and Synthesis

- **Themes and Patterns:**

Across the four reviewed papers, several common themes and patterns emerge:
Layered Approach to Security: Both Paper 1 and Paper 3 adopt a layered perspective on blockchain security. Paper 1 develops a seven-layer architecture to analyze vulnerabilities, while Paper 3 classifies attacks and mitigations based on a layered blockchain model. This approach allows for a detailed understanding of specific vulnerabilities associated with each layer of the blockchain.
Focus on Smart Contracts: Paper 2 emphasizes the security of smart contracts, specifically targeting reentrancy attacks, while Paper 1 also covers smart contract

vulnerabilities as part of its broader seven-layer framework. Both papers highlight the importance of securing smart contracts due to their critical role in blockchain functionality.

Innovative Solutions and Protocols: Papers 1 and 4 introduce innovative methods to enhance blockchain security. Paper 4's Proof of Adjourn (PoAj) protocol presents a novel consensus mechanism designed to mitigate several key attacks, while Paper 1's seven-layer model offers a new taxonomy for understanding blockchain security. These innovations aim to address existing gaps in blockchain security practices.

Mitigation Strategies: Papers 1, 3, and 4 provide mitigation strategies for identified vulnerabilities. Paper 1 offers a taxonomy that helps in developing targeted countermeasures, Paper 3 suggests specific strategies such as quantum-resistant cryptography, and Paper 4 discusses practical implementations to address transaction delays and other issues.

- **Gaps in the Literature:**

  Empirical Validation: Papers 1 and 2 lack empirical data to validate their proposed frameworks and methods. Paper 1 relies on secondary research, and Paper 2's formal verification methods may not fully account for practical scenarios. This gap limits the ability to assess the real-world effectiveness of the proposed solutions.

  Coverage of Emerging Threats: Papers 1 and 3 acknowledge but do not extensively address new and emerging vulnerabilities. Paper 3 mentions quantum computing as a future threat but lacks specific solutions for emerging vulnerabilities. Paper 4 focuses on specific attacks but does not cover all potential vulnerabilities or address scalability concerns.

  Implementation Challenges: Paper 4's discussion of the Proof of Adjourn (PoAj) protocol introduces complexity in implementation, which could affect adoption. There is a lack of detailed analysis on how PoAj performs under high transaction volumes or in large-scale networks.

- **Trends:** Emerging trends in blockchain security research highlight several key developments. Firstly, there is a notable advancement in the development and refinement of blockchain security protocols. Papers such as Paper 4's introduction of the Proof of Adjourn (PoAj) consensus protocol and Paper 3's exploration of

post-quantum cryptographic methods illustrate a trend towards innovative solutions aimed at addressing specific vulnerabilities and enhancing overall system security. These innovations are a response to the increasing complexity of blockchain networks and the evolving nature of security threats.

Another significant trend is the growing emphasis on formal verification methods. Paper 2's focus on using formal verification to address reentrancy attacks in smart contracts reflects a broader movement towards employing rigorous, mathematically sound approaches to ensure the reliability and security of blockchain applications. This trend underscores the importance of developing robust methodologies that can provide stronger guarantees of correctness and security.

Furthermore, there is an increasing recognition of the need to prepare for future threats. Papers like Paper 3, which discusses the implications of quantum computing and post-quantum cryptography, and Paper 4, which addresses complex attack vectors, demonstrate a proactive approach to emerging security challenges. This trend highlights the urgency of advancing security practices to stay ahead of potential future threats, ensuring that blockchain systems remain resilient in the face of evolving technological landscapes.

- **Synthesis:**

  Layered Security Frameworks: Both Paper 1 and Paper 3 demonstrate the value of layered frameworks in understanding and addressing blockchain vulnerabilities. By dissecting security issues across different layers, these frameworks offer a detailed view of where specific threats originate and how they can be mitigated.

  Innovative and Formal Approaches: Paper 4's PoAj and Paper 2's use of formal verification methods represent significant advancements in blockchain security. PoAj's novel consensus protocol and the formal methods proposed for smart contract security reflect a shift towards more sophisticated and rigorous solutions.

  Emerging Threats and Future Preparations: The papers collectively address current and future threats, such as quantum computing and advanced attack vectors. The focus on preparing for these threats highlights the ongoing evolution of blockchain security practices and the need for continuous innovation.

3 Discussion

- **Evaluation of the Literature:**

  The reviewed literature offers a multifaceted approach to addressing the research question: "How can blockchain systems be safeguarded against both existing and emerging cyber threats through improved structural frameworks, advanced verification techniques, and novel consensus protocols?" Each paper contributes valuable insights into different aspects of blockchain security, providing a comprehensive view of how to enhance the protection of blockchain systems.

  Paper 1: This paper provides a detailed structural framework through its seven-layer architecture, which breaks down blockchain systems into distinct layers: Application, Contract, Incentive, Consensus, Network, Data, and Physical. This layered approach is crucial for understanding and addressing vulnerabilities specific to each layer, which directly aligns with the research question by offering a structured method to safeguard blockchain systems. By categorizing risks and proposing targeted countermeasures, this framework contributes to improving structural frameworks. However, the paper's reliance on secondary research limits its ability to provide empirical evidence of the framework's effectiveness in real-world applications. While it offers a robust theoretical model, the lack of practical validation and empirical testing means that its applicability and effectiveness in actual blockchain environments remain uncertain. Additionally, the paper does not fully explore the interactions between layers or how emerging threats might impact the framework, potentially limiting its responsiveness to future developments.

  Paper 2: Paper 2 focuses on advanced verification techniques, specifically formal verification for reentrancy attacks in smart contracts. Formal verification provides a rigorous method to mathematically prove the correctness of smart contract code, making it a valuable tool for addressing a critical vulnerability. This aligns well with the research question by offering a method to improve the security of smart contracts through advanced verification techniques.

  Nevertheless, the paper's narrow focus on reentrancy attacks means that it does not address other significant vulnerabilities in smart contracts. The limitations of formal verification, such as its potential to miss practical scenarios or be resource-

intensive, are also not fully explored. This narrow scope and methodological limitations restrict the paper's contribution to safeguarding blockchain systems against a broader range of threats and in diverse real-world conditions.

Paper 3: This paper provides a thorough classification of blockchain vulnerabilities and suggests mitigation strategies, including quantum-resistant cryptography. By exploring various attack vectors and offering practical solutions, the paper addresses the research question by proposing methods to enhance blockchain security through improved structural understanding and future-proofing against emerging threats. The focus on quantum computing is particularly relevant for addressing future challenges.

However, the paper lacks a qualitative performance analysis of the proposed mitigation strategies and does not provide specific solutions for all emerging vulnerabilities. The limitations in evaluating the effectiveness of these strategies and the absence of a detailed examination of implementation challenges reduce the comprehensiveness of the proposed solutions. The paper's insights into quantum computing are valuable but need to be complemented by more practical guidance on integrating these technologies into current blockchain systems.

Paper 4: Introduces the Proof of Adjourn (PoAj) protocol, offering a novel consensus mechanism designed to address various blockchain attacks, including selfish mining and transaction delays. This innovation directly responds to the research question by proposing a new consensus protocol that aims to improve security and efficiency. The detailed implementation and evaluation of PoAj provide practical insights into its application.

However, the complexity of PoAj's two-phase verification process and its scalability under high transaction volumes pose challenges to its practical deployment. The paper does not extensively address these scalability issues or the potential network disruptions caused by its penalty system. While PoAj represents a significant advancement, its practical effectiveness and integration into existing blockchain systems remain areas for further exploration.

In summary, the literature collectively provides valuable insights into safeguarding blockchain systems by addressing various aspects of the research question. Paper 1 contributes a comprehensive structural framework, Paper 2 offers advanced verifica-

tion techniques, Paper 3 explores future-proofing strategies, and Paper 4 introduces an innovative consensus protocol. However, each paper also has limitations, such as a lack of empirical validation, narrow focus on specific vulnerabilities, and challenges in practical implementation. To fully address the research question, future research should integrate these insights with empirical testing, broader vulnerability analysis, and practical implementation considerations.

- **Gaps in Research:**

  A major gap across the papers has a lack of empirical validation. Paper 1 provides a theoretical seven-layer framework but lacks real-world case studies or practical validation to demonstrate how the framework performs in live blockchain environments. Similarly, Paper 2 relies on formal verification methods that, while rigorous, are often tested in controlled settings rather than diverse, real-world scenarios. Paper 4's Proof of Adjourn (PoAj) is theoretically robust but has not been extensively tested under high transaction volumes or in varied blockchain contexts. The absence of practical validation limits the ability to assess how well these frameworks and techniques work in practice, particularly when faced with complex, real-world blockchain deployments and evolving threats. Each paper addresses certain threats and vulnerabilities but often does not cover emerging or newly identified threats comprehensively. For example, Paper 1's seven-layer framework, while detailed, may not fully incorporate recent advancements in attack vectors or emerging technologies such as quantum computing. Paper 3 acknowledges the potential of quantum computing but lacks specific, actionable solutions for these threats. Paper 4, despite its innovative approach, does not extensively address how the Proof of Adjourn protocol handles new and unforeseen attack vectors. This limited coverage of emerging threats means that the proposed solutions may become outdated as new vulnerabilities and attack methods develop. The reviewed papers generally offer solutions within their specific domains but lack a cohesive approach to integrating these solutions across different aspects of blockchain security. For instance, Paper 1's structural framework does not fully address how advanced verification techniques from Paper 2 or novel consensus protocols from Paper 4 could be integrated into its layered model. Similarly, Paper 3's focus on quantum-resistant cryptography and Paper 4's consensus protocol do not discuss how these approaches could inter-

act or complement each other in a comprehensive security strategy. This lack of integration hampers the development of holistic solutions that combine structural improvements, advanced verification, and innovative consensus mechanisms. There is limited discussion on the practical implementation challenges of the proposed solutions. Paper 4's PoAj introduces a complex consensus protocol but does not thoroughly address the potential difficulties in integrating it into existing blockchain infrastructures. Similarly, the mitigation strategies proposed in Paper 3, such as quantum-resistant cryptography, may face significant implementation hurdles that are not fully explored. The practical challenges of adopting these advanced techniques, including resource requirements, compatibility issues, and potential disruptions to existing systems, remain unexplored. While each paper focuses on specific aspects of blockchain security, there is a lack of comprehensive analysis across different types of vulnerabilities and attack vectors. Paper 2's focus on reentrancy attacks is important but does not address other critical vulnerabilities in smart contracts. Paper 1's framework, though detailed, might not fully account for the dynamic nature of blockchain threats, including those emerging from new technologies or changes in attack methodologies. This narrow focus limits the ability to develop solutions that address the full spectrum of blockchain security challenges. There is a notable absence of quantitative performance metrics in the reviewed papers. For instance, Paper 1 does not provide metrics to evaluate the effectiveness of its proposed framework. Paper 2's formal verification methods are not quantified in terms of their practical impact on security. Paper 3 lacks a detailed performance analysis of its proposed mitigation strategies, and Paper 4 does not provide extensive performance data on the PoAj protocol's effectiveness. The absence of quantitative metrics makes it difficult to assess the relative effectiveness of different approaches and their practical impact on enhancing blockchain security. While the reviewed papers contribute significantly to understanding and addressing blockchain security, they reveal several gaps, including the need for empirical validation, coverage of emerging threats, integration of solutions, practical implementation challenges, broader vulnerability analysis, and quantitative performance metrics. Addressing these gaps is crucial for developing a comprehensive and effective approach to safeguarding blockchain systems against both existing and emerging cyber threats.

- **Implications for Future Research:**

  Future research should focus on addressing several key areas to enhance blockchain security against both existing and emerging cyber threats. Empirical validation through real-world testing of proposed frameworks, verification techniques, and consensus protocols is crucial to understanding their practical effectiveness. Additionally, expanding research to cover emerging threats, such as those posed by quantum computing and AI-driven attacks, will ensure that solutions remain relevant. Integration of security solutions across different blockchain domains, along with addressing practical implementation and scalability challenges, is necessary to develop comprehensive and adaptable defenses. A broader analysis of blockchain vulnerabilities, alongside the development of quantitative performance metrics, can provide objective measures of security effectiveness. Lastly, a multi-layered security approach that combines structural, procedural, and technical safeguards across the blockchain architecture will create more resilient solutions capable of withstanding a variety of attack vectors.

4 Conclusion

- **Summary of Key Findings:**

  The reviewed research papers have collectively highlighted the critical security vulnerabilities that persist across the layered architecture of blockchain systems. Each layer of blockchain, from the application layer to the physical layer, is exposed to unique risks that have been exploited through various attacks. The literature emphasizes the importance of adopting a multi-layered approach to security, reinforcing the need for blockchain developers to focus on safeguarding individual layers without neglecting the interactions between them. The findings reveal a concerning pattern: while blockchain is often praised for its decentralization and security, certain structural weaknesses are inherent to the technology, particularly in the areas of consensus mechanisms and smart contract vulnerabilities. For instance, the susceptibility of Ethereum's smart contracts to reentrancy attacks and other coding flaws exposes the ecosystem to significant risks. Similarly, consensus layers face challenges like 51 percent of attacks and selfish mining, which threaten

the integrity of decentralized networks. What stands out from this research is the centralization risk that continues to haunt blockchain systems. Large mining pools, centralized exchanges, and reliance on external data sources compromise the security and fundamental principle of decentralization that blockchain was designed to uphold. Despite advancements in consensus protocols like PoS and novel approaches like Proof of Adjourn (PoAj), the risk of centralization remains a substantial threat, making further decentralization a critical area for future research.

- **Reinforce the Importance of the Research Topic:**

  The research on blockchain vulnerabilities is crucial to the ongoing development and adoption of blockchain technology, particularly in industries like finance, healthcare, and supply chain management. Blockchain's potential to revolutionize data security and transparency cannot be overstated, but its success hinges on addressing the security flaws that threaten its foundation. As blockchain continues to gain traction in mainstream applications, securing it from both traditional and novel cyberattacks is of paramount importance. Moreover, as the field of computer science moves towards increased decentralization, blockchain represents a key technological frontier. The vulnerabilities identified in these studies are not merely theoretical concerns; they have real-world implications for trust, privacy, and security in decentralized systems. Ensuring that blockchain technologies can operate securely will pave the way for more robust applications, from cryptocurrencies to decentralized finance (DeFi) and beyond.

- **Suggestions for Future Research:**

  As quantum computing becomes a reality, the current cryptographic foundations of blockchain will likely be insufficient. Future research should explore quantum-resistant cryptographic algorithms and their integration into blockchain frameworks. The complexity and autonomy of smart contracts make them susceptible to coding errors and malicious exploits. More research into formal verification techniques, including automated tools for security auditing and real-time vulnerability detection, will be essential in securing smart contracts. Addressing centralization risks, particularly within mining pools and validation nodes, requires further exploration of decentralized consensus mechanisms. Concepts like PoAj show promise,

but more robust frameworks are needed to ensure that decentralization is upheld across all layers of blockchain systems. Leveraging AI and machine learning to monitor blockchain networks in real-time could help identify and mitigate attacks before they fully materialize. Research into AI-driven anomaly detection systems for blockchain could lead to more proactive defense mechanisms.

References

Dwivedi, K., Agrawal, A., Bhatia, A., & Tiwari, K. (2024, 04). *A novel classification of attacks on blockchain layers: Vulnerabilities, attacks, mitigations, and research directions.* Retrieved from `https://arxiv.org/abs/2404.18090` (arXiv.org) doi: 10.48550/arXiv.2404.18090

Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H.-N. (2022). Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access*, *10*, 6605–6621. doi: 10.1109/access.2021.3140091

Mollajafari, S., & Bechkoum, K. (2023, 01). Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy. *Sustainability*, *15*, 13401. Retrieved from `https://www.mdpi.com/2071-1050/15/18/13401` doi: 10.3390/su151813401

Sayeed, S., & Marco-Gisbert, H. (2020, 09). Proof of adjourn (poaj): A novel approach to mitigate blockchain attacks. *Applied Sciences*, *10*, 6607. doi: 10.3390/app10186607

A Appendix A: Member Contributions

Group Member	Contribution	Percentage
Nurdiyana	Assigned tasks for each member. Did formatting, critical analysis, conclusion, and participated in discussion.	30%
Affnan	Suggested topics. Did introduction, abstract, and participated in discussion.	30%
Karthekeyan	Found articles related to blockchain, PoAj, and participated in discussion.	20%
Sinehaa	Suggested topics, found articles related to blockchain, and participated in discussion.	20%

A.0.1 Group Member Contributions