Blockchain Networks Vulnerabilities: Common Exploits and Mitigation Techniques

Group Members :

NURDIYANA ATHIRAH
AHMAD ADAM AFFNAN
KARTHEKEYAN
SINEHAA A/P PARAMASIVAM

INTRODUCTION

1

Main Research Question:

How can blockchain systems be protected from cyberattacks using enhanced structural frameworks, verification methods, and consensus protocols?

2

Importance of Blockchain:

Transparency, decentralization, security potential in industries like supply chain, finance, healthcare.

3

Main Challenge:

Despite benefits, blockchain has multiple vulnerabilities at various layers (network, data, application, etc.)

1 Research Objectives 1

Assess the effectiveness of current prevention methods for blockchain security.

2 Research Objectives 2

Analyze key differences within studies on blockchain security measures.

3 Research Objectives 3

Study common vulnerabilities and patterns in blockchain attacks, focusing on consensus networks, protocols, and smart contracts.

Scope of the Review

Contract Layer

Smart contract vulnerabilities like reentrancy attacks.

Consensus Layer

Threats such as selfish mining and efficacy of PoS (Proof of Stake) vs. PoAj (Proof of Adjourn).

Data Layer

Transaction malleability, data manipulation issues.

Network Layer

Sybil attacks, peer-to-peer (P2P) communication threats.

Key Vulnerabilities (Literature Review)

Smart Contracts

Prone to irreversible bugs and reentrancy attacks.

Consensus Layer

Issues like selfish mining and 51% attacks.

Network Layer

Vulnerable to DDoS, Sybil attacks, and manipulation tactics.

Data Layer

Transaction malleability and timejacking attacks.

Mitigation Techniques

Smart Contracts

Formal verification methods, security auditing, and consistent updates before deployment.

Consensus Layer

Novel protocols like PoAj to counter selfish mining, improve decentralization.

Data Layer

Techniques like SegWit to prevent data manipulation.

Network Layer

Improved node verification and decentralized DNS services.

Critical Analysis of Reviewed Papers

- Paper 1: Introduces a seven-layer framework for blockchain security, emphasizing the importance of layer-specific countermeasures.
- Paper 2: Focuses on Ethereum smart contracts, highlighting vulnerabilities and the need for formal verification.
- Paper 3: Explores quantum computing threats and suggests quantum-resistant cryptography as a future solution.
- Paper 4: Proposes PoAj, a new consensus mechanism to mitigate attacks like 51% attacks and selfish mining.

Conclusion & Future Directions

- Current State: Blockchain offers robust potential but is limited by security vulnerabilities at multiple layers.
- Future Research: Focus on real-world empirical testing, addressing emerging threats like quantum computing, and ensuring practical implementation of new consensus mechanisms.

Thank You

@REALLYGREATSITE

Alfredo Torres

hello@reallygreatsite.com