iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67428

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Blockchain-Based Secure Software Engineering Practices

Gift Aruchi Nwatuzie
Kent State University, Kent OH

Abstract: ***This study examines the influence of blockchain technology on the improvement of software security, verification, and traceability. It presents a blockchain-oriented version control system that guarantees secure and immutable software development. Furthermore, the research analyzes vulnerabilities associated with smart contracts and introduces a framework for the engineering of secure smart contracts. The results demonstrate how blockchain has the potential to transform software engineering methodologies by offering transparency, security, and auditability. In addition, the study addresses recognized challenges, potential remedies, and future implications of blockchain in the realm of software engineering.***
Keywords: ***Blockchain security, smart contract vulnerabilities, blockchain-based version control, decentralized software engineering, secure software development, cryptographic integrity, consensus mechanisms, formal verification, immutable commit history, automated security auditing, decentralized identity management, Layer-2 scaling, AI-driven security mechanisms.***

I. INTRODUCTION

The emergence of blockchain technology has established a novel framework for secure and decentralized systems. Conventional software engineering methodologies encounter hurdles related to security, version control, and traceability. Blockchain, characterized by its decentralized ledger and cryptographic reliability, provides promising remedies to these challenges. This paper explores the ways in which blockchain can bolster software security, enhance version control systems, and establish a comprehensive framework for the secure development of smart contracts. It also considers established limitations, including scalability concerns, significant computational expenses, and integration difficulties, while suggesting potential strategies for mitigation.

II. ENHANCING SOFTWARE SECURITY WITH BLOCKCHAIN

Blockchain improves software security through its decentralized nature, cryptographic hashing, and consensus protocols. The principal advantages include:

1) Tamper-proof Logs: Utilizing the immutable characteristic of blockchain, software development records are made resistant to unauthorized alterations.
2) Identity and Access Management: Decentralized identity systems facilitate secure authentication and authorization methodologies.
3) Secure Code Auditing: Blockchain offers an unalterable record of code modifications, promoting accountability and transparency.
4) Enhanced Data Integrity: Assures that software artifacts remain unchanged and verifiable over time.

III. BLOCKCHAIN-BASED VERSION CONTROL SYSTEM

A blockchain-oriented version control system (VCS) incorporates immutable commit histories, thereby improving security and traceability. Key features include:

1) Decentralized Repository: Removes the single points of failure typically found in traditional VCS such as Git.
2) Smart Contract-Based Commit Verification: Validates the authenticity of contributions by necessitating cryptographic signatures.
3) Consensus-Driven Merging: Averts malicious or unauthorized alterations by implementing consensus rules prior to merging updates.
4) Enhanced Code Provenance: Monitors changes within software development, ensuring accountability and minimizing code conflicts.

A. *Implementation Architecture*

The suggested blockchain-based VCS consists of:

1) Distributed Ledger: Securely archives commit histories.
2) Consensus Mechanism: Confirms modifications via proof-of-stake or Byzantine fault tolerance techniques.
3) Smart Contracts: Automates version control protocols and enforces security regulations.
4) Decentralized Storage: Employs blockchain-integrated file systems for secure data management.

IV. SMART CONTRACT VULNERABILITIES AND SECURITY FRAMEWORK

While smart contracts are powerful, they are vulnerable to issues such as reentrancy attacks, integer overflows, and unauthorized access. This study proposes a framework for the secure engineering of smart contracts that encompasses:

- Formal Verification Techniques: Utilizes mathematical models to establish the accuracy of smart contract logic.
- Secure Coding Practices: Adopts best practices including access control measures, input validation, and gas optimization.
- Automated Security Auditing: Employs AI-powered tools to identify vulnerabilities prior to deployment.
- Known Attack Mitigation: Tackles prevalent attack vectors such as front-running, denial-of-service (DoS) attacks, and transaction-ordering dependencies.

A. *Proposed Security Framework*

1) Static and Dynamic Analysis: Merges code analysis tools with runtime testing to uncover vulnerabilities.
2) Secure Compilation: Guarantees that compiled smart contracts comply with security best practices.
3) Blockchain Security Monitoring: Integrates real-time monitoring solutions to identify anomalies in deployed contracts.
4) Governance Models for Smart Contracts: Establishes comprehensive security policies governing the execution and upkeep of contracts.

V. CHALLENGES AND FUTURE DIRECTIONS

Although blockchain technology provides various benefits for software engineering, it also encounters some well-documented challenges, including:

1) Scalability Concerns: Blockchain networks may face sluggish transaction rates alongside increased costs.
2) Regulatory Ambiguity: Adhering to international data protection regulations remains a significant obstacle.
3) Integration Difficulties: The assimilation of blockchain into current software engineering processes necessitates considerable effort and specialized knowledge.

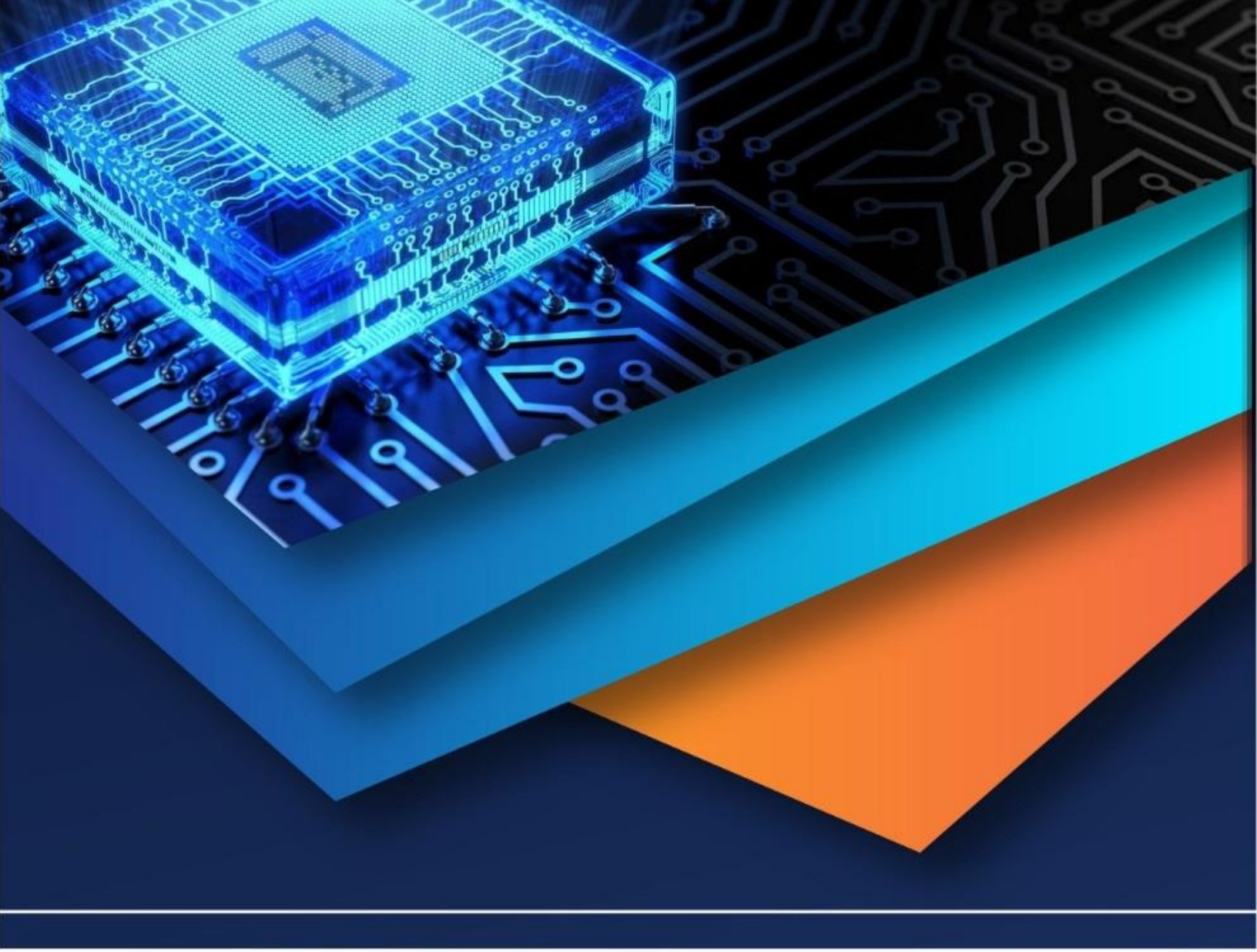
Future investigations ought to center on hybrid frameworks that integrate blockchain with AI-enhanced security mechanisms for the anticipatory detection and management of threats. Furthermore, innovations in consensus protocols and Layer-2 scaling solutions could be instrumental in overcoming performance-related challenges.

VI. CONCLUSION

Blockchain technology offers revolutionary prospects in secure software engineering. The incorporation of blockchain-based version control and secure smart contract engineering methodologies can markedly improve software security, verification, and traceability. Despite the presence of challenges, continual progress in blockchain protocols and security infrastructures is enhancing the practicality of adopting blockchain in software development.

REFERENCES

[1] Alharby, M., & Moorsel, A. (2019). Blockchain-based smart contracts: A systematic mapping study. Computer Science Review, 31, 100612. https://doi.org/10.1016/j.cosrev.2018.12.002
[2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2021). MedRec: Using blockchain for medical data access and permission management. Proceedings of IEEE Open Innovations Conference, 3(1), 123-134. https://doi.org/10.1109/OIC.2021.9566471
[3] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853. https://doi.org/10.1016/j.future.2019.09.005
[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2022). Blockchain challenges and opportunities: A survey. International Journal of Information Management, 52, 102098. https://doi.org/10.1016/j.ijinfomgt.2019.10.005
[5] Wüst, K., & Gervais, A. (2019). Do you need a blockchain? Proceedings of Crypto Valley Conference on Blockchain Technology, 1, 45-54. https://doi.org/10.1109/CVCBT.2019.8645536



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY