| Volume 02 | Issue 06 | November 2026 | ISSN: 3139-1737

International Journal of Advances and Applications in Convergent Studies & Transdisciplinary (IJ-AACST)

Bridging Disciplines, Bridging Knowledge

Aligned with the Vision of NEP 2020 and UGC Guidelines

Website: https://aacstij.org || Email: journaleditor@aacstij.org

Performance Evaluation of a SHA256-Based Verification Mechanism for Secure Blockchain Transactions

DOI: https://doi.org/10.5281/zenodo.24104442

Miss. Sheetal R. Billore[1]*, Dr. Keshao D. Kalaskar[2]

*Corresponding Author: [1] Research Scholar, Sardar Patel Mahavidyalaya, Chandrapur, Maharashtra, India,

sheetalbillore123@gmail.com

[2] Professor, Dr. Ambedkar College of Arts, Commerce and Science, Chandrapur, Maharashtra, India,

keshao_kalaskar@yahoo.co.in

ABSTRACT

The security and integrity of digital records are critical requirements in distributed information systems, particularly where electronic healthcare records and administrative documents are exchanged across multi-organizational networks. This paper presents a performance evaluation of a Python-based blockchain architecture integrating SHA-256 hashing with a secret-key verification mechanism (SHA256-VK). The system incorporates core blockchain operational components: transaction creation, block generation, proof-of-work consensus, and transaction validation. Experimental evaluations were conducted on blockchain scales ranging from 50 to 500 blocks, assessing system memory utilization, execution runtime, and average block-generation latency. Experimental results demonstrate that memory utilization scales predictably from 0.28331 MB at 50 blocks to 0.28500 MB at 500 blocks, while total execution time increases from 58.897 seconds to 78.791 seconds. The measured mean block-generation time was approximately 5.486 seconds. The findings confirm predictable resource growth within the evaluated bounds and establish baseline performance metrics for lightweight verification mechanisms in distributed ledgers.

KEYWORDS: Blockchain, SHA-256, verification secret key, SHA256-VK, data integrity, execution time, memory utilization, healthcare information systems.

1. INTRODUCTION

Digital platforms increasingly handle data that demand strict assurances regarding authenticity, traceability, and immutability. Healthcare information systems represent a key application domain where electronic health records (EHRs)—encompassing medical histories, prescriptions, laboratory diagnostics, and personal identifiers—require robust protection against unauthorized alteration and data corruption. Traditional centralized database architectures present inherent vulnerabilities, including single points of failure, centralized attack vectors, non-transparent access control policies, and inadequate auditability.

Blockchain technology offers a decentralized, append-only distributed ledger where data records are

© 2026 The Author(s). This article is published by the AACST in the IJ-AACST under the Creative Commons Attribution 4.0 International (CC BY 4.0) License. The authors retain copyright and grant AACST a non-exclusive license to publish, distribute, and archive the work.

cryptographically linked and verified across a peer-to-peer network. Cryptographic hash functions, such as SHA-256, play a crucial role in maintaining ledger integrity by generating fixed-length digests from arbitrarily sized data payloads. Because a slight modification in the underlying payload produces a fundamentally distinct output hash, hash verification provides reliable integrity validation. However, hashing alone does not provide data privacy or access control, nor does it inherently authenticate the identity of the data submitter.

To enhance transaction authentication, this study evaluates a SHA256-based verification key mechanism (SHA256-VK) integrated into a functional Python blockchain execution model. This paper analyzes the computational efficiency, runtime dynamics, and memory footprint of SHA256-VK across expanding ledger sizes, offering foundational insights into the operational characteristics of secret-key validation layers in distributed environments.

2. SYSTEM ARCHITECTURE AND RESEARCH OBJECTIVES

The primary objective of this study is to evaluate the runtime performance, scalability overhead, and computational resource consumption of the SHA256-VK blockchain prototype. The specific objectives are:

- **Formalize system workflow:** Formalize the architectural components of the SHA256-VK verification protocol.
- **Quantify memory scaling:** Quantify memory utilization profiles across dynamic blockchain capacities (50 to 500 blocks).
- **Evaluate execution runtime:** Evaluate execution time overhead as a function of block scaling.
- **Establish benchmarks:** Establish benchmarking parameters for future production-scale deployment and comparative security assessments.

The core contribution of this work lies in providing an empirical resource utilization analysis of secret-key cryptographic validation within a lightweight blockchain prototype.

3. RELATED WORK

Blockchain integration within digital healthcare and administrative management has received considerable academic focus. Sun et al. [1] proposed an IPFS-integrated blockchain model designed to secure storage and granular access to medical records. Similarly, Tanwar et al. [2] examined blockchain architectures for Healthcare 4.0 applications, demonstrating how distributed consensus enhances electronic medical record reliability. Xia et al. [3] developed BBDS, a lightweight data-sharing framework operating on cloud environments to enforce auditable access permissions.

While these studies highlight the potential of distributed ledgers in data security, real-world deployment requires balancing security mechanisms against computational performance and memory overhead. Cryptographic functions, such as SHA-256 paired with auxiliary key validation, introduce additional execution overhead that must be accurately quantified to ensure operational efficiency.

4. RESEARCH METHODOLOGY

The proposed framework is implemented using a Python environment, encompassing transaction generation, SHA-256 hashing algorithms, block header creation, proof-of-work (PoW) consensus processing, and ledger validation. The SHA256-VK layer incorporates an explicit verification secret key into the standard block validation process, verifying transaction parameters against predetermined authorization criteria before block confirmation. The performance benchmarking protocol evaluated the system across ten discrete blockchain sizes: 50, 100, 150, 200, 250, 300, 350, 400, 450, and 500 blocks. Performance metrics focused on two critical system variables:

1. Memory Utilization: Net memory allocation (measured in Megabytes, MB) required to retain ledger states and cryptographic metadata.

2. Total Execution Time: Aggregate computational time (measured in seconds, s) required to perform block creation, hashing, PoW completion, and chain validation.

5. EXPERIMENTAL RESULTS

System resource allocation was tracked across incremental block additions. Table 1 outlines the measured memory consumption, while Table 2 presents the total execution time recorded across varying chain lengths.

Table 1. Memory utilization for the SHA256-VK framework across chain sizes.

Number of Blocks	Memory Utilization (MB)
50	0.28331
100	0.28353
150	0.28365
200	0.28386
250	0.28393
300	0.28423
350	0.28426
400	0.28442
450	0.28481
500	0.28500

Table 2. Total execution time for SHA256-VK across chain sizes.

Number of Blocks	Total Execution Time (s)
50	58.897
100	60.835
150	61.835
200	61.888
250	63.829

300	63.839
350	64.839
400	69.844
450	70.867
500	78.791

As demonstrated in the experimental evaluation, memory utilization expanded by a modest margin of 0.00169 MB across the test spectrum (from 0.28331 MB to 0.28500 MB). Conversely, total execution time demonstrated a prominent increase of 19.894 seconds (from 58.897 seconds at 50 blocks to 78.791 seconds at 500 blocks). The measured average block-generation latency was recorded at approximately 5.486 seconds per block.

6. DISCUSSION

The empirical findings demonstrate distinct resource allocation trends. Memory growth remains minimal and scales linearly with ledger expansion, confirming that in-memory state tracking for small-to-medium block scales imposes negligible memory strain.

However, total execution time exhibits progressive scaling, driven largely by the cumulative computational complexity of Proof-of-Work iterations and sequential block hashing. While the inclusion of the verification secret key (SHA256-VK) strengthens identity check workflows at the transaction level, the cryptographic verification logic requires careful key lifecycle management—including secure key distribution, rotation policies, and key storage mechanisms—to prevent authentication bottlenecks in broader network setups.

7. LIMITATIONS AND FUTURE WORK

While this study establishes key baseline performance metrics, several areas remain for future extension:

- **Scalability Testing:** Future empirical evaluations should expand testing beyond 500 blocks to measure asymptotic behavior under enterprise workloads.
- **Network & I/O Latency:** Evaluation under multi-node distributed environments with simulated network jitter and transaction propagation delays is necessary.
- **Formal Security Verification:** Mathematical security proofs and adversarial threat modeling (e.g., key exposure, replay attacks, collision attempts) should be conducted to formally validate the security bounds of the SHA256-VK protocol.

8. CONCLUSION

This paper presented a performance evaluation of a SHA256-VK blockchain prototype designed for secure digital record processing. Across testing bounds of 50 to 500 blocks, memory utilization scaled gradually from 0.28331 MB to 0.28500 MB, while total execution time increased from 58.897 seconds to 78.791 seconds, alongside an average block-generation latency of 5.486 seconds. The results confirm the operational stability and

computational feasibility of integrating explicit secret-key verification mechanisms within SHA-256 hashed ledgers, offering a practical foundation for future secure distributed storage implementations.

9. REFERENCES

[1] Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access, 8, 59389–59401.

[2] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.

[3] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

[5] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data (BigData Congress), 557–564.

[6] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[7] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status and classification. Telematics and Informatics, 36, 55–81.