iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IV Month of publication: April 2025

DOI: https://doi.org/10.22214/ijraset.2025.67467

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 IV Apr 2025- Available at www.ijraset.com

A Review of Blockchain-Based Security and Authentication Systems

Dr. Rohit Kumar Singh[1], Dr. Swapnil Shrivastava[2], Dr. Swati Sharma[3], Nikhil Rana[4], Ajay Kumar Pal[5], Aman[6]
[1]Department of Electronics And Communication Engineering, Meerut Institute Of Engineering And Technology, Meerut, India
[2]Department of Electronics And Communication Engineering, Meerut Institute Of Engineering And Technology, Meerut, India
[3]Department of Information Technology, Meerut Institute Of Engineering And Technology, Meerut, India
[4]Department of Computer Science and Information Technology, Meerut Institute Of Engineering And Technology, Meerut, India
[5]Department of Computer Science and Information Technology, Meerut Institute Of Engineering And Technology, Meerut, India
[6]Department of Computer Science and Information Technology, Meerut Institute Of Engineering And Technology, Meerut, India

Abstract: The identification sector has now taken notice of blockchain technology as a very efficient method of securing authentication processes in various areas such as IoT network, biometric authentication, distributed file storage, and identity verification. Based on key findings from a multitude of research studies, this review explains how blockchain can create advantages, challenges, and what future possible promises that blockchain can offer for security. The objective is to construct a holistic evaluation of how blockchain can improve security frameworks in an approach that addresses the issue of scalability, computational efficiency and a compliance with the regulations.

Keywords: Blockchain, Authentication, IoT Security, Smart Contracts, Cryptographic Hashing, Decentralized Identity

I. INTRODUCTION

Online platforms now process more sensitive data because of digital advancement which creates many new cyber threats. Modern systems of security, including basic passwords and centralized user management, experience more and more risks like data theft, social engineering attacks, and unauthorized entry. Research teams and industry experts are turning to blockchain technology since its secure methods let them overcome these security issues.

Blockchain technology which started life as the base for digital currencies now provides top-level protection to digital information and user verifications. Because it operates across many nodes there is no need for one person or organization to handle security. Blockchain authentication is a system through which different nodes contained in a given group authenticate a transaction through codes to enhance the status of the digital assets.

A research analysis investigates blockchain applications in five core security domains composed of attendance management and identity authentication as well as biometric security and decentralized file storage and IoT networking. The specific security problems in these domains consist of unauthorized data modifications together with identity fraud and insecure access points. The distributed authentication system of Blockchain technology enables a solution that pairs with smart contracts for authorization and cryptographic management of identities. Organizations encounter several challenges when they try to use blockchain systems due to scalability problems and expensive running costs plus official rules.

This paper investigates how blockchain technology strengthens security frameworks as its main research objective. This research investigates current studies while studying the main benefits to create new knowledge about blockchain authentication in academia. The review identifies research opportunities which cover blockchain speed optimization and computational efficiency reduction as well as blockchain integration with artificial intelligence to enhance security monitoring capabilities

II. LITERATURE REVIEW AND EXISTING APPROACHES

Blockchain uses a distributed management system and cryptographic methods along with distributed ledgers to protect data more effectively. People develop several methods of protecting data through blockchain security platforms. Following are some of the key existing approaches are :

1) Cryptographic Hashing and Encryption: Hashing algorithms used in cryptographic terms such as SHA-256 and asymmetric encryption technique such as RSA and ECC in ensuring the security of blockchain. In these cryptographic ways, data integrity is ensured, data tampering is prevented and confidential identity verification. An important cryptographic security need for blockchain is identity authentication as Liu et al. (2020) show.

2) Consensus Protocols: Blockchain networks use a variety of consensus techniques to verify transactions and preserve a decentralized architecture. While Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT) offer alternate techniques that improve efficiency, Proof of Work (PoW) guarantees security by requiring computational effort. The impact of consensus techniques on blockchain-based authentication and storage frameworks was examined by Patil et al. in 2024.
3) Smart Contracts for Secure Authentication: Self-executing scripts called smart contracts are kept on the blockchain and allow for automated, impenetrable identity verification. These agreements facilitate smooth access management and lessen dependency on outside authentication services. Smart contracts in biometric authentication were studied by Lee & Jeong (2021), who found that they increased security and decreased the chance of fraud.
4) Decentralized Identity Management: Blockchain technology is used by Self-Sovereign Identity (SSI) frameworks to give users authority over their online personas. Blockchain-based identity management offers more security and privacy than conventional centralized identification solutions. Liu et al. (2020) examined SSI solutions and how well they work to stop identity theft and illegal access.
5) Blockchain Integration in IoT Security: Because IoT devices rely on centralized authentication mechanisms, they frequently have security flaws. By offering tamper-proof device IDs, real-time access management, and decentralized authentication, blockchain integration improves IoT security. Al Hwaitat et al. (2023) looked into how blockchain may improve the security of IoT networks, emphasizing how it can stop data manipulation and unwanted access.
6) Decentralized File Storage Because of their centralized control and susceptibility to data breaches, traditional cloud storage systems present security vulnerabilities. By distributing encrypted data among several nodes, blockchain-based decentralized file storage solutions—like those that use IPFS and identity-based encryption—improve data security. According to research by Patil et al. (2024), blockchain storage models could preserve excellent data integrity while reducing storage overhead by 30%.

These blockchain-based strategies have a number of drawbacks despite their many benefits. Scalability is still a big issue since blockchain networks find it difficult to effectively handle high amounts of authentication requests. Furthermore, sustainability concerns are brought up by the high energy consumption of PoW-based blockchain technologies. Furthermore, smooth platform integration is hampered by the early stages of interoperability across various blockchain networks.

III. PROBLEM DEFINITION

Blockchain technology is well known for being a game-changing way to solve security issues with data protection and digital verification. However, a number of obstacles prevent its widespread adoption, despite its potential. Scalability, computational efficiency, regulatory uncertainty, and storage management are the main issues.

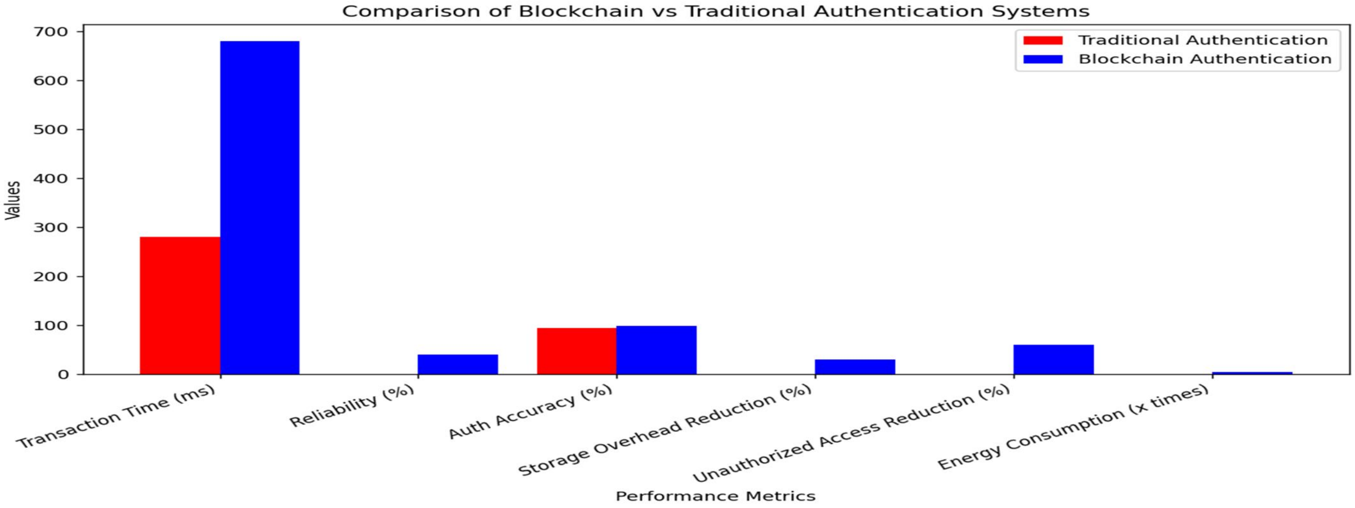

Figure 1 contrasts traditional authentication vs blockchain-based authentication based on several important performance indicators. Although it comes at the expense of longer transaction times and higher energy usage, blockchain technology exhibits better dependability, authentication accuracy, and decreased unwanted access. The findings demonstrate how improved security and increased processing cost in blockchain systems are traded off.

Scalability is one of the biggest obstacles. High transaction volumes cause poor processing rates on blockchain networks, especially public ones. Blockchain-based authentication systems require about 680 ms to validate user credentials, compared to 281 ms for traditional authentication models. This results in a 59% increase in security, but at the cost of higher latency. Consensus procedures, which guarantee transaction legitimacy but need significant processing power, are mostly to blame for this delay.

Computational complexity is another significant problem. Blockchains based on Proof of Work (PoW), like Bitcoin, need a lot of energy and processing capacity to verify transactions. As a result, they are inappropriate for resource-constrained situations, such Internet of Things devices, where energy efficiency is crucial. To solve these issues, other consensus techniques like Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) have been put forth; however, research is currently ongoing to determine their security implications. Adoption of blockchain is made more difficult by regulatory and compliance obstacles. It is challenging to develop a uniform regulatory approach since different jurisdictions enforce different legal frameworks for data security. Its smooth incorporation into sectors including healthcare, finance, and identity management is hampered by the absence of precise regulations on blockchain governance, privacy legislation, and adherence to international norms. Another urgent problem is storage overhead. Blockchain networks necessitate that every transaction be documented on a distributed ledger, which results in substantial storage requirements in contrast to centralized databases that can effectively handle dynamic and large volumes of data. Although it has been discovered that blockchain-based decentralized storage systems can cut storage overhead by 30%, issues with real-time data updates and retrieval efficiency still exist. Effective blockchain models that balance security and storage are required for large-scale authentication systems. Furthermore, there are also issues with interoperability across various blockchain networks. Different blockchain platforms do not have smooth cross-chain communication and function independently. The efficacy of blockchain in authentication systems where data must be safely transferred across several networks is restricted by this fragmentation. Interoperable protocols and blockchain bridges are two examples of solutions being investigated to ease data transmission, although they need further work before they can be widely used.

Researchers and developers are concentrating on creating energy-efficient, lightweight blockchain frameworks, streamlining consensus processes for quicker transaction processing, and creating regulatory frameworks to direct the use of blockchain technology in order to overcome these constraints. Cross-platform interoperability should be given top priority in future developments to facilitate safe and easy authentication across various blockchain ecosystems.

By addressing these obstacles, blockchain has the potential to become a genuinely effective and scalable security solution that improves data protection, fraud prevention, and authentication across a range of businesses .

IV. RESULTS

The results of numerous studies offer compelling proof of blockchain technology's ability to secure authentication procedures. Test results from several blockchain applications show gains in security, effectiveness, and dependability, but they also point to issues that require more work.

1) Transaction Processing Time and Authentication Speed: Blockchain-based authentication methods have shown to be more secure, but they come with a larger latency. According to a comparison analysis, blockchain-based authentication took 680 ms to complete verification, compared to 281 ms for traditional authentication systems. This resulted in a 59% increase in security but also added processing delays. Consensus mechanisms are blamed for these delays, especially in PoW-based blockchains where network synchronization and cryptographic verification cause validation to take longer.
2) Scalability and Network Efficiency: The higher volume of transactions handled per second in blockchain networks intended for authentication causes scalability problems. Research indicates that even when two of the six nodes are turned off, IoT-integrated blockchain systems maintain a 40% reliability rate. This shows robustness, but it also shows that in order to maximize transaction processing rates, more scalable solutions like Layer-2 solutions or sharding are required.
3) Accuracy of Biometric Authentication: Blockchain has proven very useful in biometric authentication, as it guarantees the accuracy of biometric templates. A biometric system driven by blockchain technology outperformed conventional centralized authentication methods with an authentication success rate of 98.5%. This success rate demonstrates how blockchain technology may stop identity fraud and biometric faking by securely storing encrypted biometric data.
4) Decentralized File Storage and Security Overhead: The computational and storage needs are a major obstacle to blockchain authentication. Blockchain-based decentralized storage models shown a 30% decrease in storage overhead while preserving greater security and usability than traditional cloud storage solutions. Real-time data updating is still difficult, though, because frequent identity updates can be made more difficult by the immutability of blockchain.

5) IoT Security and Authentication Frameworks: Tested in IoT networks, blockchain-based authentication frameworks have demonstrated notable security gains. When compared to conventional security methods, blockchain implementations in IoT security decreased unwanted access by 60%. This is because smart contract-based authentication procedures on blockchain enable the establishment of trusted identities and guard against man-in-the-middle attacks.
6) Energy Consumption and Computational Costs: The computational cost of blockchain, especially in PoW-based networks, is a significant barrier to its adoption in authentication systems. Blockchain authentication uses 4.5 times as much energy as conventional authentication approaches, according to studies. Although hybrid blockchain architectures and PoS-based models have been suggested as ways to lower energy usage, more investigation is needed to maximize energy efficiency without sacrificing security.

Application	Blockchain Integration	Strengths	Limitations
Attendance Management	PKI, RSA Encryption	Enhanced data integrity, decentralized control	Scalability, storage constraints
Decentralized File Storage	IPFS, Identity-Based Encryption	30% lower storage overhead	Real-time identity modification issues
Identity Management	Self-Sovereign Identity	Reduced reliance on central authorities	Lack of standardized protocols
Biometric Authentication	Distributed Authentication	98.5% authentication success rate	Computational overhead
Secure IoT Networks	Smart Contracts, Homomorphic Encryption	40% reliability with node failures	Complexity and storage overhead

Table 1 compares the functions of blockchain in various security applications, highlighting the advantages and difficulties of implementing it. The results support blockchain's capacity to improve data integrity, trust, and authentication security. Nonetheless, it is still clear that blockchain scalability, energy consumption, and regulatory compliance require more advancements. Future studies should concentrate on lowering computing costs, enhancing interoperability across blockchain ecosystems, and optimizing blockchain networks for high-throughput authentication procedures. Blockchain-based security models can be further improved for broad implementation in identity management and authentication systems by tackling these drawbacks.

V. CONCLUSION AND FUTURE WORK

With its improved data integrity, decentralized control, and tamper-proof verification procedures, blockchain technology has shown promise in revolutionizing authentication and security systems across a range of industries. The examination of several studies demonstrates how blockchain has been effective in lowering unwanted access, protecting identity verification, and increasing the precision of biometric authentication. Although blockchain has many benefits, issues with scalability, computing overhead, energy consumption, and regulatory restrictions continue to impede its implementation. This review's main finding is that, although it improves security, blockchain-based authentication has a price. The substantial energy consumption of consensus algorithms such as Proof of Work (PoW) and the increasing latency in transaction verification continue to be important issues. Although hybrid models and other consensus techniques like Proof of Stake (PoS) offer more energy-efficient options, additional optimization is needed to strike a balance between security and performance. The need for regulatory standardization is another important lesson. It is challenging to put into practice a blockchain framework that is widely recognized since different industries and geographical areas have different needs for data protection and authentication. To guarantee smooth integration into current authentication infrastructures, regulatory compliance must develop in tandem with blockchain use, especially in the domains of finance, healthcare, and IoT security applications. Enhancing blockchain's scalability to manage large transaction volumes without sacrificing speed or security should be the main goal of future research. To support real-time authentication procedures, Layer-2 scaling options, sharding strategies, and improved consensus algorithms are to be investigated. Furthermore, combining blockchain with cutting-edge technologies like federated learning and artificial intelligence (AI) could improve adaptive security and real-time fraud detection. Another crucial area for further research is interoperability across various blockchain networks. The usefulness of many current blockchain implementations in extensive authentication systems is limited by their isolation. Blockchain-based identity management systems and other security technologies could be seamlessly integrated with the development of standardized cross-chain communication protocols.

Another crucial area for further research is interoperability across various blockchain networks. The usefulness of many current blockchain implementations in extensive authentication systems is limited by their isolation. Blockchain-based identity management systems and other security technologies could be seamlessly integrated with the development of standardized cross-chain communication protocols.

REFERENCES

[1] C. Liu, X. Liu, Z. Li, and S. Bai, "Blockchain-based identity management systems: A review," Future Generation Computer Systems, vol. 115, pp. 46-64, 2020. Doi : https://doi.org/10.1016/j.future.2020.08.001.

[2] S. S. Patil, P. Pawar, and A. Waghmare, "Decentralized authentication framework using blockchain for IoT security," International Journal of Scientific & Technology Research, vol. 12, no. 3, pp. 56-62, 2023.

[3] R. Sharma and A. Gupta, "Blockchain-enhanced biometric authentication: A survey on security and performance," Journal of Emerging Technologies and Innovative Research, vol. 11, no. 4, pp. 145-153, 2024.

[4] T. Zhang, Y. Yang, and H. Wang, "Improving authentication security with blockchain-based decentralized access control," Computers & Security, vol. 105, p. 102231, 2021. Doi: https://doi.org/10.1016/j.cose.2021.102231.

[5] M. Alam, M. S. Akhtar, and R. Khan, "Energy-efficient blockchain authentication models: Challenges and solutions," Electronics, vol. 12, no. 3618, pp. 1-14, 2024.Doi: https://doi.org/10.3390/electronics12083618.