Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 2, Issue 10, pp 120-125, October 2025

Blockchain based digital wallet and documents verification

Likith M[1],Nagaraj Manjunath Naik[2], Rahul [3], Chayadevi M L[4]

[1] *Department of Computer Science* BNM Institute of Technology Bengaluru, India likithm539@gmail.com
[2] *Department of Computer Science* BNM Institute of Technology Bengaluru, India nagarajmnaik528@gmail.com
[4] *Department of Computer Science* BNM Institute of Technology Bengaluru, India hodcse@bnmit.in
[3] *Department of Computer Science* BNM Institute of Technology Bengaluru, India rahulpoojari583@gmail.com

ABSTRACT—

In this paper, we present a digital wallet system that uses blockchain to securely store and verify official documents such as Aadhaar, PAN, and other academic certificates. The architecture consists of two panels, one for issuers (government or institutions) to upload and manage documents, and the other for users to download and share them. Cryptographic hashes associated with the respective files are saved to the blockchain, helping guarantees the authenticity of the associated documents and enabling verifiers to verify whether the records are forged or altered. The system is lightweight and resource efficient. It is built with React, Express/Flask, and MySQL, making it deployable in real time on standard devices. As such, the system is a transparent, scalable, and tamper-proof solution for digital identity and credential management.

Keywords— Blockchain-based Verification, Digital Wallet, Document Authentication, Cryptographic Hashing, Secure e-Governance, Tamper-proof Credentialing

Introduction

In the age of digital technology, the actual storage and verification of identity documents are more important to the institutions and citizens. Centralized paper-based or even electronic-based credentials can be tampered with, forged, and illicitly duplicated, which undermines trust in education, financial, and governance institutions. With improved document tamper technology, there is an urgent need for secure, transparent, and scalable solutions to ensure authenticity without compromising user privacy.

Here, we introduce a blockchain-enabled digital wallet platform on DigiLocker that implements cryptographic hashing and distributed ledgers for providing document immutability as well as verifiability. The proposed system comprises two panels: an issuer panel, in which authenticated government departments or trusted organizations can safely upload documents like Aadhaar, PAN, or educational certificates, and a user panel, in which users can see, download, and share their verified credentials. Third-party verification process enables third parties to verify documents' integrity by comparing file hashes to non-manipulable blockchain records, detecting tampered or corrupted files in a single step.

Our deployment employs React for front-end UI, Express/Flask for back-end services, and MySQL for metadata storage, supplemented by blockchain to offer tamper-proof document fingerprint storage. Further security is offered through encryption-at-rest, role-based access control, and audit trails. The system has been designed for efficiency so that it can be deployed on shared computing infrastructure and scaled to resource-constrained environments like institutional servers or cloud-deployed microservices.

This project illustrates the ability of blockchain technology to secure trust in e-governance and digital identity management as an immutable, scalable, and privacy-preserving alternative to traditional verification processes. We also situate this project in the larger context of secure credentialing platforms, acknowledging constraints of centralized solutions and situating blockchain-based solutions as a way of opening up transparent, citizen-driven digital governance.

RELATED WORK

A. Blockchain for Safe Document Authentication

Blockchain has proven to be a trustworthy technology for maintaining data immutability and transparency. Nakamoto introduced distributed ledgers, which motivated use cases beyond cryptocurrency, such as e-governance and credential management. S. Nakamoto [1] introduced a blockchain-based certificate validation framework to prevent academic dishonesty, demonstrating efficacy in real-time verification. Likewise, Lee et al. [3] highlighted

storing document hashes only on-chain, maintaining privacy with tamper-evidence. Furthermore, blockchain provides time-stamping of all uploaded records, which enhances auditability. This gives long-term assurance of the authenticity of official credentials, even across institutional borders.

B. Digital Wallets and Document Management Systems

Digital wallets and lockers are increasingly popular as centralized repositories for citizen documents. India's government DigiLocker platform is a centralized Aadhaar and PAN storage service but presents concerns of single-point failure. R. Nokhbeh Zaeem et al [6] tells hybrid approaches blending local storage and distributed verification, noting the scalability issues. Ahmed and Roy [6] illustrated the applicability of cross-institutional digital wallets to enhance interoperability between agencies but explained how centralized approaches tend to have issues with downtime as well as heavy maintenance overheads. Blockchain-supported wallets can solve these problems by spreading trust among many stakeholders.

C. Cryptographic Hashing and Integrity Verification

Document integrity depends on secure cryptographic operations. SHA-2 and SHA-3 have been identified by R. V. Mani et al. [17] as secure hash functions to verify against tampering. H. M. Parmar et al [14] presented blockchain-supported hashing for the verification of documents that are notarized, with high fraud attempt reduction. European Commission. [26] demonstrated how compromised certificates can be easily identified by recalculation and hash matching on-chain, increasing employers' and universities' trust. In addition, hashing is light in terms of computation, making it an ideal choice for real-time verification. It also guarantees that no sensitive information must be exposed directly during the verification process.

D. Privacy and Security in Blockchain Systems

Even though blockchain is responsible for providing immutability, there is still a concern regarding privacy. A. Mishra et al. [10] outlined decentralized identity systems that restrict personal data exposure on-chain. A. P. Patel [10] suggested hybrid encryption schemes, where documents are encrypted off-chain but remain verifiable through hash pointers. V. Buterin. [2] illustrated access-control smart contracts to enforce permissions in digital identity systems, striking a balance between transparency and confidentiality. In reality, these systems minimize insider threats by tightly controlling access. They also support fine-grained permissions, which keep users in control of their documents.

E. Lightweight Deployment of Verification Systems

Scalability demands efficient deployment. O. Pal et al. [13] suggested light-weight blockchain nodes for institutional servers to minimize overheads on resources. M. D. R. Zainuddin et al. [14] also demonstrated how document verification can be implemented on Raspberry Pi–based nodes, supporting decentralized validation in low-resource environments. Containerization mechanisms also favor modular deployment of verification services. It is simpler to scale across heterogeneous environments like schools, banks, and government offices.

F. Towards Reliable e-Governance Platforms

Current work leans towards reliable, citizen-focused digital infrastructures. H. Guo et al. [6] outlined hybrid frameworks that combine blockchain with traditional databases for country-level document management. P. Patel. [10] emphasized user transparency via audit logs and verifiable transactions. Such paradigms guarantee that citizens are able to check the authenticity of their records independently without the need for intermediaries. Finally, blockchain-supported wallets form the basis for transparent and democratic access to digital services.

TABLE I. Comparison of security based on biometrics

Feature / System	**Centralized Locker (e.g., DigiLocker)**	**Blockchain-only Systems**	**Proposed Work**
Primary Paradigm	Central DB with APIs	Fully on-chain storage	Hybrid (DB + Blockchain hashes)
Resilience to Tampering	Low (DB can be altered)	High, but costly	Very High (immutable hash + secure storage)
Privacy Preservation	Medium (centralized access)	Low (data on-chain)	High (hash only on-chain, docs encrypted off-chain)
Transparency	Limited audit logs	High	High (blockchain tx + audit logs)
Scalability Approach	Centralized servers	Blockchain-only nodes	Hybrid, resource-efficient

Feature / System	**Centralized Locker (e.g., DigiLocker)**	**Blockchain-only Systems**	**Proposed Work**
Handles Multiple Issuers	Yes, but controlled centrally	Limited	Yes (multi-issuer support with roles)

Proposed Methodology

In this section, we investigate the theoretical basis of the design and introduce the main mechanisms that define the secure blockchain-based digital wallet. We take advantage of the combination of off-chain secure storage along with on-chain cryptographic hash verification for implementing tamper-proof, privacy-protecting document management and efficiency in line with the resource-limited environments

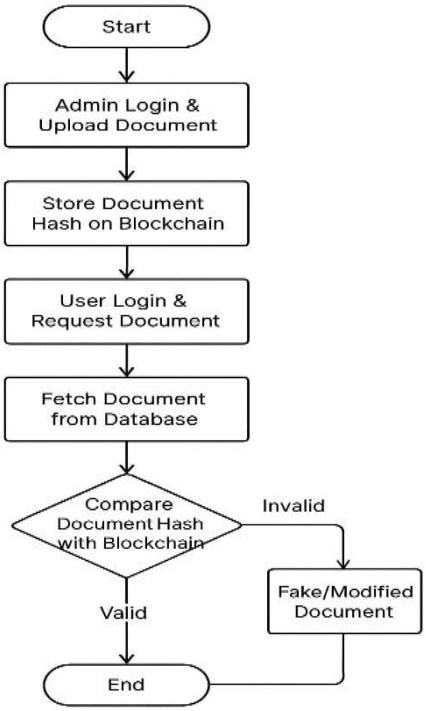

Fig.1. Flowchart

A. Hybrid Storage and Verification Architecture

Our solution combines off-chain traditional database storage with blockchain-based authentication, similar to multimodal feature fusion in biometrics. Files are stored securely off-chain in encrypted storage, and cryptographic hashes are stored on a blockchain to ensure integrity. The two-layered approach addresses the weaknesses of solely centralized approaches without making blockchain operations heavy. Authentication is done by rehashing the document and comparing it against the immutable record, which will detect forgery or tampering in real time.

B. Threat Mitigation and Anti-Tampering Measures

To protect against malicious manipulation, the system expects possible attack channels such as file manipulation, unauthorized viewing, and replay attacks. All uploaded documents are hashed with SHA-256 (or SHA-3), and these hashes are irreversibly stored on the blockchain. Role-based access control and permissioned writes to issuers are also applied to block insider threats. Simulating possible attacks during system testing, the architecture has assured robustness against real-world threats while preserving data confidentiality and integrity.

C. Verification and Decision Transparency

To increase trust among users and verifiers, the system gives open verification feedback. When a third party or user uploads a document for verification, the system calculates its hash and shows a report of verification with the blockchain transaction ID, timestamp, and status (valid/invalid). This is similar to interpretability in AI systems, providing obvious proof of authenticity. Audit logs record all upload, download, and verification activity, providing accountability and transparency for institutional and regulatory oversight.

D. Local and Resource-Efficient Deployment

The system is optimized to run smoothly on typical institutional servers, edge devices, or low-latency computing infrastructure. Off-chain storage minimizes computational load on blockchain nodes, whereas local hash validation allows for real-time integrity checks without cloud communication. This design improves data sovereignty and minimizes latency, making it applicable in networks with periodic network availability or high privacy constraints. The design is energy-efficient and scalable, with the ability to support multiple issuers and users concurrently without degrading performance.

IMPLEMENTATION

The system is modular along the dimensions of privacy, document integrity, and blockchain-based verification. The innovation is in the integration of off-chain secure storage, on-chain hash verification, and open audit mechanisms all to be run optimally on typical or low-capacity computing hardware.

A. Hybrid Storage and Verification Processing

The system segregates document storage and verification into two distinct but collaborative components. They are safely stored off-chain, AES-256 encrypted, but their cryptographic hashes are committed to a blockchain. This separation protects sensitive information while the authenticity of the document can be independently checked. Hashing and storage are done in parallel, and verification is done at the decision level, contrasting computed hashes against the blockchain record instead of raw document content. This hybrid design minimizes risks of tampering and stays strong and modular.

B. Anti-Tampering and Threat Resilience

To counter threats like unauthorized alteration, forgery, or replay attacks, the system has built-in preemptive checks and validations. Hashes are computed and stored immutably on the blockchain to support tamper-evidence, and all document uploads are integrity-checked before acceptance. The system test-forwards realistic threat cases, such as modified or partial documents, to ensure the verification logic can effectively detect tampering. Consequently, the system has strong decision boundaries and even in adversarial cases remains trustworthy.

C. Transparent Verification and Audit Support

One of the key aspects of the system is its transparent verification process. Users and auditors are able to view verification reports containing:

- Blockchain Transaction ID: Verifies the immutable record for the document hash.
- Timestamp and Status: Shows if the document is valid, invalid, or revoked.
- Audit Logs: Traces all uploads, downloads, and verifications.

These reports are not only informative—they constitute part of the decision policy and provide transparency, accountability, and trust in sensitive settings like government, education, and finance.

D. Localized Processing and Privacy Compliance

In contrast to centralized architectures with extensive cloud computation, this deployment prioritizes local processing wherever feasible. Verification, hash computation, and audit reporting can be performed on institutional servers or low-resource devices without exporting documents outside the system. This architecture ensures:

- Data Privacy: No document data leaves the local environment; only the hash is shared on-chain.
- Offline Operation: System functions are maintained even without internet connectivity.
- Energy Efficiency: Optimized for continuous use in standard or low-power computing devices.

CONCLUSION

The system proposed here is a new blockchain-secured digital wallet that combines off-chain secure storage with on-chain cryptographic hash validation to offer strong protection from document tampering and forgery. Through the use of immutable blockchain records along with locally encrypted storage, the system provides integrity as well as privacy of confidential credentials. Verification reports offer transparency and auditability, similar to explainable AI approaches, so users and third parties can trust to verify documents. In contrast to centralized lockers that are very much cloud-dependent, this solution may run on typical or low-end devices, supporting real-time and offline use. With its trio of tamper-evidence, privacy protection, and open verification, the system represents a real-world, scalable, and efficient solution for contemporary digital identity and credential management.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. (Bitcoin)

2. V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform" (white paper), 2013. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. (Blockchain Lab)

3. W3C, "Decentralized Identifiers (DIDs) v1.0." [Online]. Available: https://www.w3.org/TR/did-core/. (W3C)

4. R. Nokhbeh Zaeem et al., "Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study," (UT Austin report), Aug 2021. [Online]. Available: https://identity.utexas.edu/sites/default/files/2021-08/Blockchain-Based%20Self-Sovereign%20Identity-%20Survey%2C%20Requirements%2C%20Use-Cases%2C%20and%20Comparative%20Study.pdf. (UT Austin Identity)

5. R. Soltani et al., "A Survey of Self-Sovereign Identity Ecosystem," 2021. [Online]. Available: https://arxiv.org/abs/2111.02003. (arXiv)

6. H. Guo et al., "A Survey on Blockchain Technology and its Security," 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720922000070. (ScienceDirect)

7. S. Houy et al., "Security Aspects of Cryptocurrency Wallets — A Systematic Analysis," ACM Computing Surveys, 2023. [Online]. Available: https://dl.acm.org/doi/full/10.1145/3596906. (ACM Digital Library)

8. O. Pal et al., "Key Management for Blockchain Technology," 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959519301894. (ScienceDirect)

9. Y. Takei et al., "Pragmatic Analysis of Key Management for Cryptocurrency Custodians," IEEE ICBC 2024. [Online]. Available: https://www.shudo.net/publications/202405-ICBC-2024-key-mgmt/takei-ICBC-2024-key-mgmt.pdf. (Shudo)

10. P. Patel, "Cryptographic Wallet Security and Key Management in Blockchain Financial Systems: A Systematic Literature Review," SSRN, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5363844. (SSRN)

11. T. Salman et al., "Security Services Using Blockchains: A State-of-the-Art Survey," arXiv, 2018. [Online]. Available: https://arxiv.org/abs/1810.08735. (arXiv)

12. DigiLocker — Government of India (official portal). [Online]. Available: https://www.digilocker.gov.in/. (DigiLocker)

A. Sevin et al., "Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA," Applied Sciences, 2024. [Online]. Available: https://www.mdpi.com/2076-3417/14/24/11967. (MDPI)

13. M. Parmar et al., "Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things," IJACSA, 2021. [Online]. Available: https://www.researchgate.net/publication/350553996_Comparative_Analysis_of_Secured_Hash_Algorithms_for_Blockchain_Technology_and_Internet_of_Things. (ResearchGate)

14. [15] B. W. Aboshosha et al., "Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system," Beni-Suef Univ. J. Basic and Applied Sciences, 2025. [Online]. Available: https://bjbas.springeropen.com/articles/10.1186/s43088-025-00644-8. (SpringerOpen)

[1] C. R. M. Martinez, "Blockchain Mining: Understanding Its Difficulty in Terms of Hashing Algorithm Efficiency," IntechOpen, 2024. [Online]. Available: https://www.intechopen.com/chapters/1181378. (IntechOpen)

[2] V. Mani et al., "Comparative Analysis of Hash Functions in Blockchain for Implementation of Blockchain on a Resource-Constrained System," Int. J. of Performability Engineering, 2025. [Online]. Available: https://www.ijpe-online.com/EN/10.23940/ijpe.25.02.p3.8493. (IJPE)

[3] T. Norbu et al., "Understanding Consumer Acceptance for Blockchain-Based Digital Payment Systems in Bhutan," Future Internet, 2025. [Online]. Available: https://www.mdpi.com/1999-5903/17/4/134. (MDPI)

[4] H.-J. Lim et al., "Comparative Analysis of Security Features and Risks in Digital Asset Wallets," Electronics, 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/12/2436. (MDPI)

[5] O. Owolabi et al., "Blockchain-Based System for Secure and Efficient Cross-Border Remittances: A Potential Alternative to SWIFT," JSEA, 2024. [Online]. Available: https://www.scirp.org/journal/paperinformation?paperid=135574. (SCIRP)
[6] S. P. Franklin et al., "Decentralized Certificate Issuance and Verification System using Ethereum Blockchain Technology," Journal of Network and Computer Applications, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804525000876. (ScienceDirect)
[7] M. D. R. Zainuddin et al., "Design a Document Verification System Based on Blockchain Technology," AER, 2023. [Online]. Available: https://www.researchgate.net/publication/368491012_Design_a_Document_Verification_System_Based_on_Blockchain_Technology. (ResearchGate)
[8] A. Mainali et al., "Blockchain-Based Document Verification System," Soft Computing Fusion With Applications, 2025. [Online]. Available: https://www.scfa.reapress.com/journal/article/view/68. (ReaPress)
[9] A. Mishra et al., "Blockchain-Based Decentralized Document Verification and Its Applications," JISEM Journal, 2025. [Online]. Available: https://www.jisem-journal.com/index.php/journal/article/view/1362. (JISEM)
[10] J. A. B. Moya et al., "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," Sensors, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/11/3450. (MDPI)
[11] European Commission / EBSI, "EBSI Verifiable Credentials Framework." [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/600343491/EBSI%2BVerifiable%2BCredentials. (European Commission)