International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 35-42 March 2026-Sept 2026 www.csjournals.com

Blockchain Digital Identity Verifier: Stores User Credentials for Privacy-Preserving Access

Anjali, Dr. Sneha, Dr. Anupam Bhatia
Deptt. of Comp. Sc. and Application, Chaudhary Ranbir Singh University, Jind, Haryana, India

Abstract

Digital identity verification is critical for accessing various online services. Still, traditional identity management systems depend on centralized databases at risk of unauthorized access and identity theft. This paper introduces a Blockchain Digital Identity Verifier designed to securely store user credentials and provide access in a privacy-preserving manner using blockchain technology to overcome these challenges. It brings together DIDs, Issuer service, smart contracts, cryptographic hashing as well as IPFS-based off-chain storage to create a secure and decentralized (IAM) system. Storing full user credentials on the blockchain is avoided, instead encrypted credentials are stored off-chain. Cryptographic agreements ensure transparency and data integrity to verify credentials, manage access control.

The proposed system provides improved security and enables selective information for user privacy, reduces trust in intermediaries and lowers the risk of credential fraud. It can be used in several sectors like banking, medical sector, education, e-governance. It also provides a secure, transparent, and scalable way to verify digital identities.

Keywords: Blockchain, Digital Identity Verification, Decentralized Identity (DID), Verifiable Credentials, Smart Contracts, IPFS, Privacy-Preserving Access.

Introduction

At this time, digital IDs are used from opening a bank account and applying for government services. These services can be accessed through an identification process known as digital identity verification. This is achieved through presenting documents (like Aadhaar cards, PAN cards, or passports) to a central body, that holds and validates these documents.

However, this existing model has a significant drawback all your personal information is held in one centralized location making it at risk of misuse. Whenever you disclose your identity to a new service, you have limited control over how it will be used.

A blockchain is a digital ledger distributed among multiple computers that is tamper-proof and transparent. This technology is used in a Blockchain Digital Identity Verifier, which verifies user credentials without sharing the actual personal data with third parties. Only a cryptographic proof, a mathematical fingerprint that proves your credentials, is recorded on the blockchain. Meanwhile, real information remains along with you in a secure off-chain database. This concept is based on (SSI), which is the idea of individuals that should control their own

Blockchain technology provides a feasible way to address such obstacles. Its key features like immutability, decentralization, cryptographic security, and transparency, is suitable for digital identity verification systems.

A blockchain-based digital ID Verifier can enable users to keep their credentials securely, with control over their personal information. The verification process can be executed on a blockchain network instead on a central authority, which reduces the risks of data manipulation. In addition, privacy-preserving techniques also ensure that only information necessary for verification is shared.

The purpose by this paper helps to create a blockchain user identity verifier that securely stores user credentials and allows access in a privacy-preserving manner. The proposed approach aims to enhance security, increase user privacy, reduce dependence on centralized systems.

Literature Review

Ref. No.	Authors	Proposed Work	Key Findings	Limitations
[1]	Jamal et al.	Introduced blockchain-based identity verification provide secure system for digital identity verification.	Found SSI to be an emerging identity framework that gives users complete control over their identity information.	Scalability and real-world deployment challenges were not fully addressed.
[2]	Aydar et al.	Developed a blockchain-based digital identity verification and record-sharing system.	Enabled secure authentication and reliable access to digital records while increasing user trust.	Integration with existing systems and interoperability remain challenging.
[3]	Alammary et al.	Carried out a survey on IDM systems.	Identified blockchain as a suitable solution for decentralized, transparent, and immutable identity management.	Scalability, interoperability, and adoption barriers still exist.
[4]	Ishmaev	Explored blockchain-based identity systems from sovereignty, privacy, and ethical perspectives.	Highlighted the importance of decentralized identity in improving user control and privacy.	Privacy protection, ethical concerns, and regulatory compliance require further attention.
[5]	Čučko and Turkanović	Performed a review study on DID and SSI.	Found SSI to be an emerging identity framework that provides users full	Practical implementation and widespread adoption need further research.

			complete control over their identity information.	
[6]	Ahmed et al.	Presented a comprehensive survey of blockchain-based identity management and SSI ecosystems.	Concluded that SSI provides increased security as well as privacy compared to traditional identity systems.	Interoperability and large-scale deployment remain open research issues.
[7]	Schardong and Custódio	Carried out a systematic review and taxonomy of SSI systems.	Explained key SSI concepts such as DIDs, Verifiable Credentials, and blockchain trust models.	Focused mainly on taxonomy rather than implementation or performance evaluation.
[8]	Ding and Sato	Proposed a SSIaaS architecture.	Demonstrated secure identity sharing while preserving user ownership and privacy.	Limited discussion of scalability and practical deployment challenges.
[9]	Reece and Mittal	Studied SSI applications in authentication across different domains.	Showed that SSI offers flexible, privacy-preserving, and secure authentication mechanisms.	More validation is required for large-scale real-world applications.
[10]	Salem et al.	Analyzed blockchain-enabled biometric identity management systems.	Combined blockchain security with biometric authentication to improve identity verification and prevent unauthorized access.	Biometric privacy concerns and computational overhead remain significant challenges.

Problem Statement

• The existing approach to identity management is a centralized system that faces security risks, privacy concerns, or lack of user control over personal identity.

• Traditional authentication methods are weak, so credentials increase the risk of unauthorized access and fake verification.

• Existing identity verification processes are time-consuming because they involve manual verification.

• Users are not fully in control and ownership of their digital identities, so resulting in trust and transparency problems.

Research Gap

To enhance security, privacy as well as trust on identity checking process, multiple researchers have introduced digital identity system using blockchain-based identity management system and (SSI) frameworks. Despite current systems, there are still a few drawbacks exists such like dependency on central authorities, users not having much control and privacy issues.

Still, many blockchain-based ID solutions face scalability and interoperability problems. They can also face problems with secure credential sharing, credential standardization and integration with conventional identity systems.

The identified research gaps include:

• Blockchain-based identity systems need a large storage capacity with the growth of identity records over time, which leads to storage and management issues.

•A large number of existing systems fail to ensure efficient and reliable verification of digital credentials.

•There are no effective mechanisms for credential sharing and ownership of digital identity solution using blockchain.

•Challenges related to user control and privacy protection for personal identity data is not sufficiently covered.

•Current systems are limited when the number of transactions of identities continue to grow.

Research Objectives

This study focuses on achieving the following main objectives:

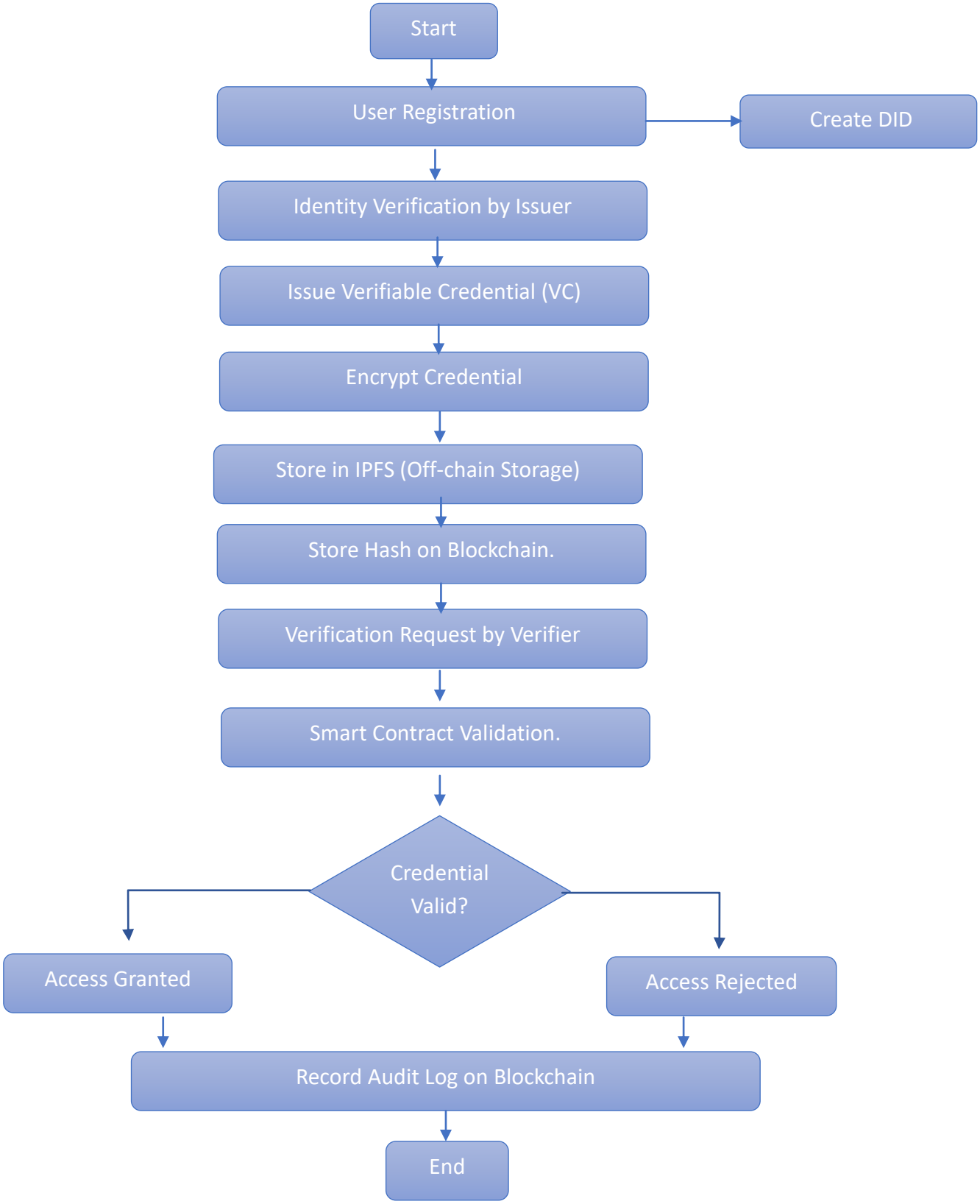
1. To perform an analysis of blockchain identity systems and (SSI).
2. To analyze performance gap in conventional centralized identity management systems.
3. To design a safe as well as decentralized verification process mechanism using distributed ledger.
4. Increase privacy as well as security of digital identity data.
5. To allow users to manage their data with control.
6. To identity fraud through blockchain authentication.
7. To access authentication and credential security standards.
8. To examine challenges like scalability, interoperability, and privacy issues in current blockchain identity frameworks.

Proposed System Framework

The framework in proposed decentralized digital identity system is implementing for creating a secure, decentralized, and privacy-preserving secure identity management system. This proposed framework supports the current identity verification methods based on centralized

databases, DIDs, VCs, smart contracts, cryptographic verification techniques.It maintains that users have control over their trusted entities and they can validate them without revealing unnecessary details. Credential hashes are safely registered on the blockchain network during encryption documents are saved in decentralized off-ledger.

Workflow

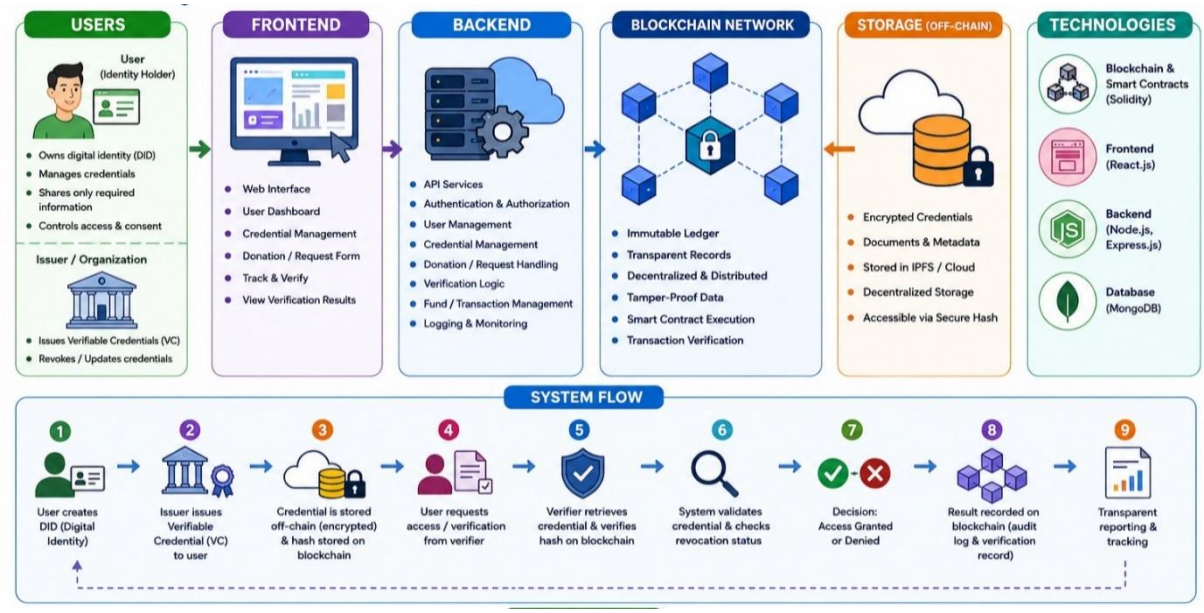


International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 17 • Issue 2 pp. 35-42 March 2026-Sept 2026 www.csjournals.com

Existing Identity Control System

Most of the existing identity control systems are generally non-distributed and use third-party organizations to keep and validate user details. Users have restricted control over their personal identity data, and organizations manage most of the identity verification processes. These systems may be at risks of security, data breaches, privacy concerns, and unauthorized access because identity information is stored in centralized databases.

The verification of digital identities and credentials manual checking makes the process time consuming. There is also a risk of identity fraud, fake credentials, and misuse of personal information. Current systems are less secure, less decentralized, and do not provide efficient management of digital identities.



Benefits For the Proposed System

The proposed blockchain-based identity control system offers a secure as well as decentralized digital identity management solution. It increases user protection by giving them control to share their personal information. This system enables transparent and tamper-proof identity verification blockchain technology. It also decreases the identity fraud and increases trust between users and organizations.

Conclusion & Scope for Future Work

Thus, this paper presents a distributed ledger-based digital identity verifier to ensure secure, decentralized, and management framework. Traditional identity management systems commonly experience problems like centralized data storage, identity theft, unauthorized access, and limited user control over personal data. These challenges decrease user trust and increase the risk of data breaches.

The proposed system uses blockchain technology to securely verify digital identities. Smart contracts perform the identity verification workflow and control access permissions without depending on a central authority. User credentials are securely maintained in off-chain storage, while only their cryptographic hashes are recorded on the blockchain. This technique protects sensitive user information while enabling secure and tamper-proof identity verification.

The proposed framework increases security and minimizes identity fraud. It also improves user privacy, and provides users high control over their digital credentials. It also provides a safe and transparent identity verification mechanism that can be implemented in different sectors like medical sector, education, banking, e-governance, as well as enterprise authentication.

Blockchain login system, like biometric recognition technology, can also be included to enhance user authentication. As well as AI and ML is able to utilized automatically detectings fake identities and suspicious activities.

Furthermore, the proposed framework can also facilitate cross-chain identity interoperability, allowing users to verify their digital identities across multiple blockchain based networks. This improvement will increase scalability, interoperability, and adoption of decentralized identity solutions in large-scale real-world applications.

References

[1] Jamal, A. S. N. Syahirah, R. A. A. Helmi, M.-A. Fatima, Blockchain-Based Identity Verification System, Faculty of Information Sciences and Engineering, Management & Science University, Shah Alam, Malaysia, 2019.

[2] M. Aydar, S. Ayvaz and S. C. Cetin, “Towards a Blockchain Based Digital Identity Verification, Record Attestation and Record Sharing System,” arXiv preprint arXiv:1906.09791, 2019.

A. Alammary, S. Alhazmi, M. Almasri and S. Gillani, Blockchain Based Identity Management Systems: A Review, Journal of Network and Computer Applications, vol. 166, 2020, p. 102731.

G. Ishmaev, “Sovereignty, Privacy, and Ethics in Blockchain-Based Identity Management Systems,” Ethics and Information Technology, vol. 23, no. 2, pp. 239–252, 2021.

[5] Š. Čučko and M. Turkanović, “Decentralized and Self-Sovereign Identity: Systematic Mapping Study”, IEEE Access, vol. 9, pp. 139009–139027, 2021.

M. R. Ahmed, A. K. M. Muzahidul Islam, S. Shatabda and S. Islam, “Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey,” IEEE Access, vol. 10, pp. 113436–113481, 2022.

[7] F. Schardong and R. Custódio, “Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy”, Sensors, vol. 22, no. 15, p. 5641, 2022.

[8] Y. Ding, H. Sato, Self-Sovereign Identity as a Service: Architecture in Practice, arXiv preprint arXiv:2205.08314, 2022.

[9] M. Reece and S. Mittal, "Self-Sovereign Identity in a World of Authentication: Architecture and Domain Use Cases," arXiv preprint arXiv:2209.11647, 2022.

[10] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-Based Biometric Identity Management," vol. 27 of Cluster Computing (2020). 3741–3752, 2024.