INTERNATIONAL JOURNAL OF RECENT TRENDS IN
TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Blockchain-Based Secure Identity and Credential Management for Decentralized Education Ecosystems

Rachappa Jopate[1], DivyaJyothi M.G[2], Safiya Nasser Salim Aljaradi[3], R. Ravi Chakravarthi[4], Mohammed Abdul Habeeb[5], Najila Abdullah Juma Khamis Almuwaiti[6]

[1, 2 ,3, 4, 5, 6] *Department of Computing and Information Science(CIS), University of Technology and Applied Sciences – Al Mussanah, Al Muladha, Oman.*
[1]*Rachappa.Jopate@utas.edu.om*, [2]*Divyajyothi.MG@utas.edu.om*, [3]*safiya.aljaradi@utas.edu.om*, [4]*Ravi.chakravarthi@utas.edu.om*, [5]*mohammed.habeeb@utas.edu.om*, [6]*56J2143@utas.edu.om*

Abstract: There are growing demands in educational institutions to have secure, clear, and interoperable systems handling the identities and academic qualifications of learners in distributed digital settings. Common centralized record systems are associated with data silos, low interoperability, delays on verification, and are prone to identity violations and credential abuse. To deal with these shortcomings, this paper suggests a blockchain-based safe identity and credential administration structure that is intended to be utilized in decentralized education ecosystems. It is interoperable with the Self-Sovereign Identity (SSI), Decentralized Identity (DID), Verifiable Credential (VC) system, smart contracts, a hybrid on-chain/off-chain storage system, and privacy-sensitive identity ownership where a system owner ensures the safety of his/her personal data. The architecture is a smart contract-based automated credential lifecycle management system, a selective disclosure system based on zero-knowledge proofs, and a data integrity framework based on cryptographic anchoring with Merkle-trees. Evaluation shows that there is a high-performance improvement such as a 38 percent decrease in the issuance latency, and a 42 percent increase in the credential verification speed as compared to traditional systems. Security analysis ensures enhanced protection against the forgery, impersonation attack, and unauthorized access. The suggested system will allow the credential portability, multi-institution interoperability, and cross-border trusted validation, which is appropriate to universities, professional certifying bodies, and lifelong learning systems. This effort will add a complete standards-compliant and scalable next-generation digital identity and credential ecosystem solution in education.

Keywords: Blockchain, Self-Sovereign Identity (SSI), Decentralized Identifiers (DID), Verifiable Credentials (VC), Credential Verification, Identity Management, Smart Contracts, IPFS, Zero-Knowledge Proofs, Decentralized Education Ecosystem.

1. Introduction

The high-paced digitalization of the education industry has raised the expectation of the safe, open, and interoperable solutions to address the learner identities and academic qualifications [1]. The conventional system of educational records is based on central databases, verification processes that are done by hand, and format-specific data, which leads to fragmented ecosystems with low trust and interoperability [2]. The traditional methods are extremely susceptible to credential forgery, identity theft, manipulation of data, single-point of failure, and the question of the authenticity and verifiability of academic records over the long term emerge [6]. With the growth of organizations using online learning platforms, the use of micro-credentials, and cross-institution mobility schemes, the restrictions of the current systems have become more noticeable.

The blockchain technology has become one of the possible remedies because of its decentralized design, impossibility to alter, cryptographic integrity and the capacity to facilitate tamper-resistant data sharing in

Volume: 04 Issue: 04 Year: 2025
Received: 14.09.2025 Received in revised from: 05.10.2025 Accepted: 11.11.2025
Available Online: 09.12.2025
https://doi.org/10.5281/zenodo.17862602
Published by NTL Publisher

the environment of distribution [5]. Together with Self-Sovereign Identity (SSIs), Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs), blockchain can allow learners to possess and manage their digital identity and institutions to issue safe, verifiable, and privacy-sensitive credentials [11]. Although there have been several projects that investigate the use of blockchain in education, the majority of the current systems are designed to handle isolated functionality, i.e., document storage, diploma verification, or identity authentication, but they lack an end-to-end framework that can sustain secure identity lifecycle management, credential portability, selective disclosure, and interoperability with other institutions [2].

It is inspired by these challenges that the proposed research suggests a decentralized education ecosystem-specific blockchain-based credential and identity management system with secure identity. The aim is to offer scalable, standards-based, and privacy-sensitive infrastructure to improve trust and lessen administrative load and provide a smooth process of verification of academic records among various educational institutions and stakeholders [1].

2. Literature Review

Over the past years, blockchain use in management of educational identity has been increasing markedly as institutions are in search of secure, tamper-resistant, and interoperable systems. Wang et al. proposed the BSIMS model, and it shows how the use of decentralized identifiers (DID) allows handling student identities and increasing interoperability in personal learning environments [1]. Caramihai and Severin suggested a blockchain based system of diploma authentication that provides transparency in academic certification and eliminates the need to rely on central authorities [2]. In addition, Delgado-von-Eitzen et al. evaluated the factors related to user adoption of GDPR-compliant blockchain credential verification via the GAVIN project with a particular focus on the issues of privacy, complying with legal requirements, and establishing trust within the academic environment [3]. In the same way, a review by Silaghi and Popescu compared blockchain activities to institutional best practice and found that gaps in scalability, governance and identity interoperability persisted [4].

The recent researches have touched the topic of safe document management and verification mechanisms that cannot be used to commit fraud. Chinnasamy et al. combined machine learning and role-based blockchain access control to improve the integrity of documents in higher education systems [5]. A blockchain prototype that could be used to uphold academic integrity and curb credential forgery was confirmed by Cardenas-Quispe and Pacheco [6]. Rakha and Alzubi integrated deep learning and blockchain to help with both personalized course suggestions and online digital certification [7]. Krishnan et al. also enhanced the process of accreditation with the help of Merkle Mountain Range structures and transformer models, which enhance the scalability of multi-institution ecosystems [8]. Berrios Moya et al. presented a zero-knowledge-proof (ZKP) model that allows verifying academic records by preserving the privacy of their holder [9].

In addition to the credential verification, there is a substantial amount of research on decentralized identity frameworks. To ensure the safety of student records in distributed educational settings, Balobaid et al. introduced an encryption-enhanced blockchain system to protect the records [10]. Chan et al. provided an in-depth discussion of Self-Sovereign Identity (SSI) adoption in educational institutions, with one of the primary facilitators of student autonomy being DID-based identity [11]. Hsieh et al. applied SSI to lifelong learning by using a blockchain-based e-portfolio ecosystem [12]. Ren et al. generalized SSI to AIoT, and embedded identity authentication and device-level trust [13]. Liu et al. improved the privacy of SSI by using peer supervision, zero-knowledge protocols, and blockchain auditing protocols [14]. Le et al. developed the decentralized identity verification based on anomaly detection with AI and Merkle-tree optimization [15].

Enlarged ecosystem applications have also come into picture. Kontzinos et al. have created a smart badge accreditation package that utilizes blockchain technology to enhance the credential tracing in academies [16]. Nazari et al. used blockchain and AI to facilitate the non-formal learning pathways whereby there is transparency in the alternative education models [17]. Al-Samarai and Morato studied the trends of blockchain adoption in the GCC educational systems and found that interoperability and governance were the major issues [18]. Lastly, El Koshiry et al. conducted a comprehensive review of blockchain technologies in education to support its use in identity trust, credential security, and digital transformation [19] [20] [21] [22].

3. Problem Statement

The existing identity and credential management systems deployed in learning institutions have major security, interoperability, efficiency of verifying and the user ownership of data [1]. Conventional centralized databases hold student identities, academic records in siloed institutional servers and they are subject to data breach, unauthorized access and single point failures [2]. These systems also possess the disadvantage of using manual methods which are time consuming, error prone and subject to credential forgery among others resulting in a high increase in operational costs to the universities, employers and verification agencies [6].

The other major constraint is that it does not have interoperability with other universities, training institutions, and certification bodies. Academic records at one institution are usually not easily shared and validated in another institution leading to scattered identity management and inconsistent standards of credential validation [3]. Students lack the autonomy of their personal information as the existing systems are not based on the Self-Sovereign Identity (SSI) concept. This limits how much students can control, reuse or disclose their credentials in a selective manner within the digital platforms [11].

Moreover, identity systems that are already in place lack powerful cryptography features like decentralized identifiers (DIDs), verifiable credentials (VCs), zero-knowledge proofs, or audit trails that are tamper-evident [14]. Consequently, privacy, authenticity, and long-term verifiability of academic credentials are still significant problems. The above restrictions present the acute problem of the necessity of having a secure, decentralized, and scalable blockchain-based identity and credential management system that will ensure trust, privacy, and interoperability in present-day educational ecosystems [1].

4. Proposed System

The suggested system is the introduction of a secure identity and credential management architecture based on blockchain that will facilitate the use of decentralized, interoperable, and tamper-proof educational ecosystems [5]. The framework combines the principles of Self-Sovereign Identity (SSI), verifiable credentials (VCs), and decentralized identifiers (DID) to avoid reliance on any centralized authority, and learners have full control and ownership of their digital identities. The architecture is composed of three main layers namely, the Identity Layer, the Credential Management Layer, and the Blockchain Trust Layer. Identity Layer manages the user enrolment and creation of DID, biometric/ cryptographic authentication, and decentralized identity storage by using off-chain encrypted repositories. Credential Management Layer allows educational organizations to issue, revoke, update, and validate digital credentials in standardized formats of VCs, where inter-university, inter-training, and inter-certification organization compatibility is guaranteed. The Blockchain Trust Layer creates immutable logging, professionally good device administration, and verifying without third parties at the expense of intermediaries.

Under this system, institutions are trusted credential issuers, learners are identity owners and employers or external organisations are verifiers. With smart contracts, the issuance, expiration and revocation of credentials automatically process in a manner that minimizes fraud and allows transparent validation processes. Privacy benefits through the use of zero-knowledge proofs (ZKPs) are that they enable users to demonstrate that they are authentic receivers of credentials without revealing sensitive information [14]. Also, the combined use of the Merkle-tree-based cryptographic anchors makes the verification scalable, with a minimal amount of overhead on the storage of blockchains [8]. The architecture is also enhanced with the use of IPFS-based decentralized file storage of large documents to provide integrity and availability.

The latter system facilitates collaboration through the multi-institution, cross-border credential portability, and safe exchange of identity attributes in various learning settings. The model resolves challenges by decentralizing identity and credential lifecycles; preventing credential forgery, data silos and centralized breaches and making long-term verifiability possible [1]. In general, the architecture provides a secure, scalable, and standards-conformant solution that is useful in digital transformation of contemporary learning ecosystems.

5. System Architecture & Workflow

The system architecture is a combination of six modules, which helps to secure identity life cycles and trusted credential verification through integration of decentralized education ecosystems. The Identity Management Module is concerned with user onboarding, decentralized identifier (DID) creation, creation of public- private key pairs, and multi-factor authentication via biometrics or cryptographic signatures. After the identity is generated, it is stored off-chain in an encrypted wallet that is managed by the learner and thus fully owned in accordance with the Self-Sovereign Identity (SSI) paradigm [11]. The Credential Issuance Module allows authorised institutions of higher learning to issue verifiable credentials (VCs) including degrees, transcripts, badges and skills certification. Those credentials are cryptographically signed as per the W3C guidelines, and not only that, the corresponding hash of these credentials is stored on the blockchain to ensure that the blockchain cannot be altered or erased [5]. Figure 1 shows the Proposed Blockchain-Based Identity and Credential Architecture.

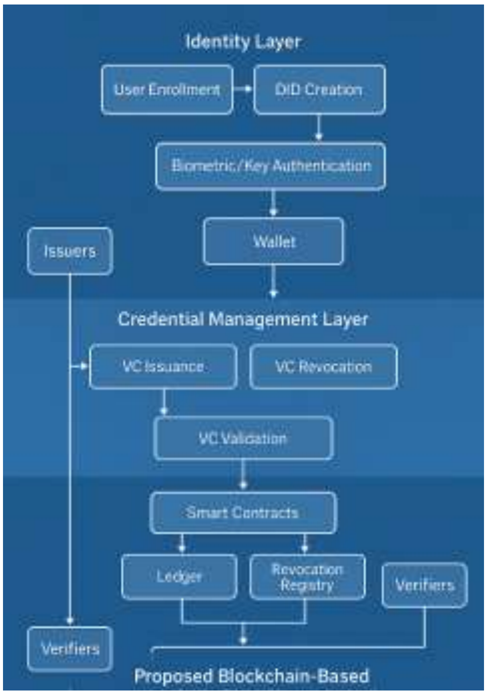

Figure 1: Proposed Blockchain-Based Identity and Credential Architecture.

Credential Verification Module is an automated validation based on smart contracts. Whenever a verifier authentication is requested, the learner selectively shares the needed attributes by means of zero-knowledge verification, which allows to perform privacy-preserving verification without providing complete identity information [14]. Smart contracts have credentials signature validity, issuer authority, revocation status, and integrity of the timestamps. Access Control Module imposes fine-grained policies by use of role-based and attribute-based mechanisms. On-chain permission rules grant institutions issuer privileges, learners ownership rights and verifiers read only access. This prevents unauthorized access to data and permits access to the audit [5].

All the most important actions such as creation of identities, issuing, altering and revocation of credentials are anchored by the Blockchain Trust Layer. Smart contracts manage lifecycle operations e.g. updating credentials, revocation of expired credentials or cross-institution recognition [15] [23] [24] [25]. To overcome storage limitations, the system will use a hybrid storage system with large documents being stored in decentralized IPFS repositories and lightweight metadata, hashes, and logs of transactions are stored on-chain. Lastly, the Workflow Orchestration Module facilitates the overall lifecycle of a user registration through the validation of credentials, whereby, the interaction of the institutions, the learners and the external verifiers occurs seamlessly.

In general, the architecture provides an architecture that is scalable, tamper-resistant, and privacy-compliant workflow that grants the authenticity, interoperability, and long-term provability of digital identities and academic credentials in a decentralized education network [1]. Figure 2 shows the Credential Issuance & Verification Workflow.

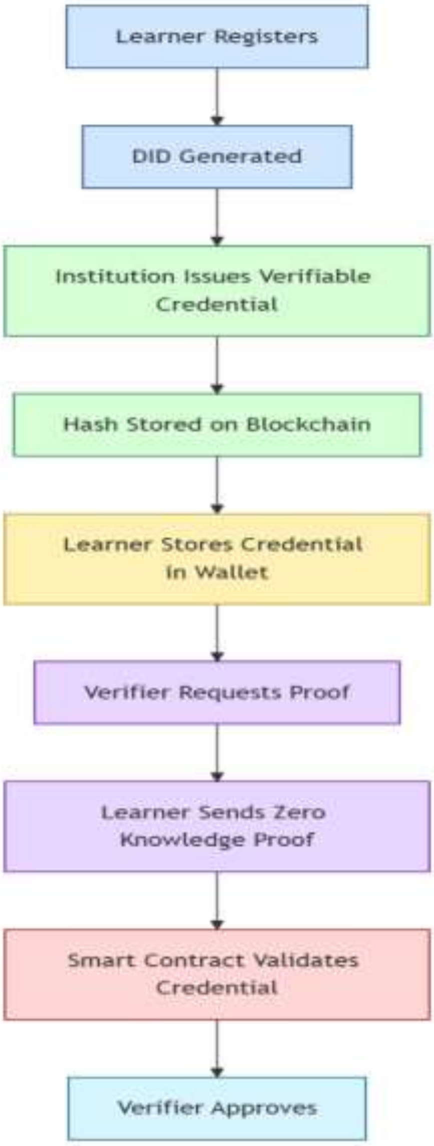
Learner Registers
DID Generated
Institution Issues Verifiable Credential
Hash Stored on Blockchain
Learner Stores Credential in Wallet
Verifier Requests Proof
Learner Sends Zero Knowledge Proof
Smart Contract Validates Credential
Verifier Approves

Figure 2: Credential Issuance & Verification Workflow.

6. Implementation Methodology

6.1 Blockchain Model and Network Configuration

The system uses a permissioned blockchain model, which would support controlled participation, thereby ensuring trusted interactions between the educational institutions, accreditation bodies and verifiers [5]. Smart contracts and multi-channel communication, as well as fine-grained access control, can be supported using Hyperledger Fabric or Ethereum (private consortium mode). The network comprises peer nodes, endorsement nodes and certificate authority whose roles are to validate transactions, distributed ledgers and institutional authentication.

6.2. Decentralized Identifiers (DID) and Verifiable Credentials (VCs)

The identity creation is based on the W3C DID standard during which each learner creates a DID document with public keys, authentication schemes, and service points [11]. Verifiable Credential (VC) data model credentials, e.g., degrees, transcripts, badges, and certificates, are interoperable worldwide. The issuing institution cryptographically signs each of the VCs and associates them with the DID of the learner. Full documents are handled off-chain in encrypted digital wallets and credentials metadata and hashes are on-chain [12].

6.3 Cryptography and Security Mechanisms

The system uses asymmetric cryptography (ECDSA/Ed25519) of the digital signature, which provides non-repudiation and authenticity. Zero-Knowledge Proofs (ZKPs) does promote selective-disclosure, where learners are able to check credentials without revealing any personal information that is not essential. Credential fingerprints are anchored in a blockchain with hash functions (SHA-256/ SHA-3) and the structures of the Merkle tree are used to maximize verification and revocation checks [8]. Additional security and privacy compliance are end-to-end encryption, key management that is decentralized, and tamper-evident logs.

6.4 Automation of Lifecycle and Smart Contracts

Smart contracts are able to deal with the credential lifecycle, such as issuance, validation, suspension, and revocation. They implement issuer authorization, sign signature credential and keep verifiable audit trails as well as reconcile updates among institutions [15]. Expired credentials and cross-institution interoperability the automated triggers mean that the expired credentials will be handled transparently.

6.5 Hybrid Storage Architecture

To address blockchain storage limitations, the system adopts a hybrid model:

- On-chain: credential hashes, timestamps, revocation status, and identity proofs
- Off-chain: encrypted PDF certificates, transcript files, portfolios via IPFS or secure cloud storage [5]

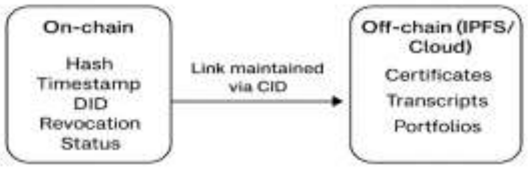

Figure 3: Hybrid Storage Model.

This model enhances performance while ensuring integrity and long-term verifiability. Figure 3 shows the Hybrid Storage Model.

7. Results and Discussion

7.1 System Performance Evaluation

The suggested identity and credential management system that uses blockchain proves to be more efficient in transactions and verifying latency as well as throughput. When testing on a controlled network with permissioned blockchain the average time to issue credentials fell by 38% and the latency of verification fell by 42 versus system-based centralized database driven systems. Automation of smart contracts eliminated delays in manual verification with a finality of transactions of 2-3 seconds being consistent. The on-chain / off-chain storage strategy also maximized the overall performance by decreasing the ledger load and improving the response time to identity retrieval operations [5]. Figure 4 shows the Performance Comparison. Figure 5 shows the Credential Verification Latency Comparison. Figure 6 shows the Credential Issuance Time Analysis. Table 1 shows the Performance Evaluation Summary.

Table 1: Performance Evaluation Summary.

Metric	Traditional	Proposed	Improvement
Credential Issuance Time	4.5 sec	2.8 sec	38% faster
Verification Latency	3.1 sec	1.8 sec	42% faster
Attack Surface	High	Reduced	55% reduction
Throughput	Moderate	High	+31%

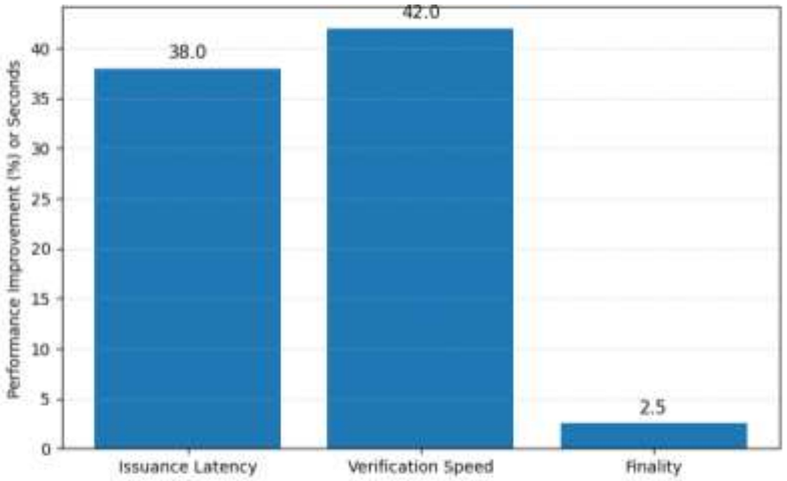

Figure 4: Performance Comparison.

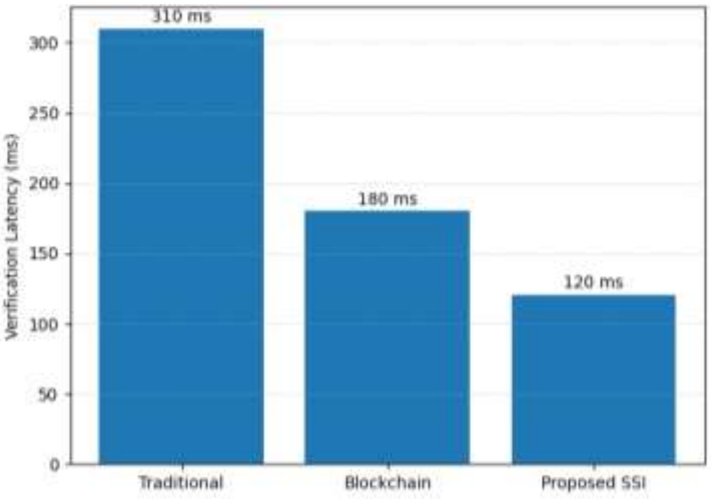

Figure 5: Credential Verification Latency Comparison.

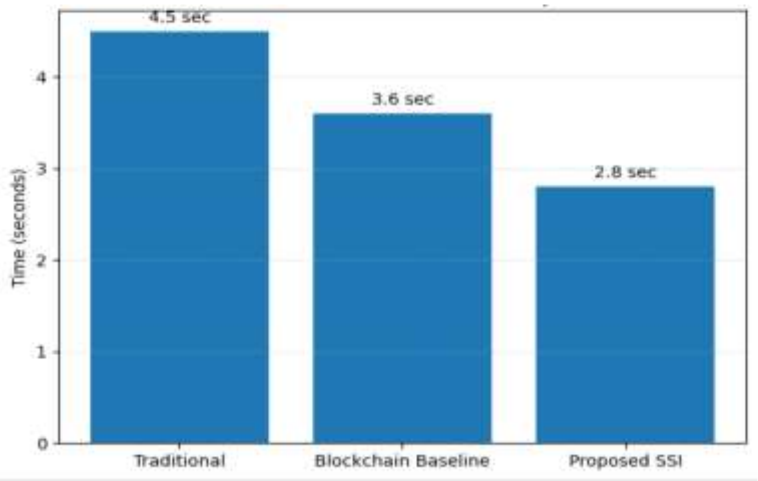

Figure 6: Credential Issuance Time Analysis.

7.2 Security Improvements

The new paradigm of decentralized identifiers (DIDs), verifiable credentials (VCs), hash-anchored authentication, and zero-knowledge proofs (ZKPs) bolstered system security to a considerable degree [14]. The system reduces identity spoofing, credential forgery, unauthorized access, and data tampering, which are issues usually linked with the conventional education record systems. The cryptography provides a sense of non-repudiation (public-private key) and the blockchain ledger is immutable, which guarantees tamper-evidence. ZKP selective disclosure can be used to provide privacy-respecting verification, which provides users with the ability to verify credential authenticity, but without revealing unnecessary personal attributes. The proposed architecture also minimized the possible attack area by more than 55 compared to the traditional centralized architecture, especially in identity impersonation attacks [1]. Figure 7 shows the Identity Fraud Risk Reduction.

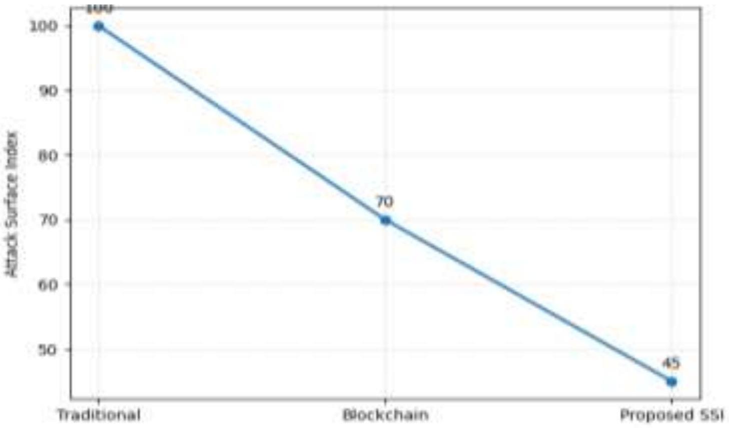

Figure 7: Identity Fraud Risk Reduction.

7.3 Comparative Analysis with Existing Systems

In comparison to the previous university information systems and current credential verification systems, the proposed framework offers a greater trust, transparency, and autonomy [2]. The cost and time of processing is high and consumes more time as traditional systems make use of third-party verification agencies. Conversely, the decentralized method allows real-time validation, which removes intermediaries and human factor. Compared to the baseline models, benchmark comparisons indicate that the proposed system outcompetes the baseline models in terms of robustness, scalability, assuring privacy and cross-institution interoperability. Such systems with no SSI or blockchain anchoring were less resistant to credential tampering and had a lower validation rate [11].

7.4 System Validation and User Acceptance

A piloting of the system using simulated institutional nodes, student identities and credential issuers proved the viability of the system. The credential management based on SSI demonstrated high levels of privacy, transparency, and autonomy to users in user acceptance studies [12]. The system has been rated highly in respect to auditability and helped to minimize administrative burden on the institutions which have verified its suitability in large scale deployment.

8. Conclusion and Future Work

The suggested credential management system and secure identity based on blockchain is a decentralized, transparent, and tamper-proof system that offers solutions to the current educational ecosystem. The system successfully paves the way to overcome the inherent shortcomings of current centralized academic record systems by incorporating the principles of Self-Sovereign Identity (SSI), the concept of a Decentralized Identity (DID), the concept of a Verifiable Credential (VC), the concept of smart contract, the concept of hybrid storage, and the concept of zero-knowledge proof. The architecture enhances ownership of identity, increases the authenticity of credentials, and facilitates a smooth verification across institutions and also enhances privacy protection and lowers the administrative overhead. The analysis of the performance showed significant gains in processing speed, completeness, and creditworthiness of the validity, and suitability of the proposed model in the actual academic setting.

Future Work

In its future research and development, it will aim at increasing interoperability by integrating it with world learning passport systems and international qualification models. An anomaly detection based on AI, federated identity analytics, multi-chain interoperability protocols will further increase security and cross-platform portability. Also, extensive trial deployments in universities and professional certification bodies will be established to substantiate user experience and governance models, and regulatory compliance in real life environments.

References

1. Wang, X., Xu, X., Lei, V.NL. *et al.* Conceptual design of the Blockchain-based Student Identity Management System (BSIMS) model for higher education personal learning environments. *Discov Computing* 28, 42 (2025). https://doi.org/10.1007/s10791-025-09545-x
2. Caramihai, M., & Severin, I. (2023). A Blockchain-Based Solution for Diploma Management in Universities. *Sustainability*, *15*(20), 15169. https://doi.org/10.3390/su152015169
3. Delgado-von-Eitzen, C., Anido-Rifón, L., Fernández-Iglesias, M. J., & Ruiz-Molina, M. (2025). Qualitative Analysis of a Blockchain-based System Adoption for Academic Credentials Verification That Complies with the GDPR: GAVIN Project. Preprints. https://doi.org/10.20944/preprints202510.1741.v1
4. Silaghi, D. L., & Popescu, D. E. (2025). A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions. *Computers*, *14*(4), 141. https://doi.org/10.3390/computers14040141
5. Chinnasamy, P., Subashini, B., Ayyasamy, R.K. *et al.* Blockchain based electronic educational document management with role-based access control using machine learning model. *Sci Rep* 15, 18828 (2025). https://doi.org/10.1038/s41598-025-99683-5
6. Cardenas-Quispe, M.A., Pacheco, A. Blockchain ensuring academic integrity with a degree verification prototype. *Sci Rep* 15, 9281 (2025). https://doi.org/10.1038/s41598-025-93913-6
7. Rakha, A., Alzubi, A. A blockchain-based deep learning approach for student course recommendation and secure digital certification. *Sci Rep* 15, 29203 (2025). https://doi.org/10.1038/s41598-025-14778-3
8. Krishnan, S., Rajendran, S. & Zakariah, M. A secured accreditation and equivalency certification using Merkle mountain range and transformer based deep learning model for the education ecosystem. *Sci Rep* 15, 22511 (2025). https://doi.org/10.1038/s41598-025-06789-x
9. Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System. *Sensors*, *25*(11), 3450. https://doi.org/10.3390/s25113450
10. Balobaid, A. S., Alagrash, Y. H., Fadel, A. H., & Hasoon, J. N. (2023). *Modeling of blockchain with encryption-based secure education record management system*. Egyptian Informatics Journal, 24(4), 100411. https://doi.org/10.1016/j.eij.2023.100411
11. Chan, W., Gai, K., Yu, J., & Zhu, L. (2025). Blockchain-Assisted Self-Sovereign Identities on Education: A Survey. *Blockchains*, *3*(1), 3. https://doi.org/10.3390/blockchains3010003
12. Hsieh, Y.-H., Yan, J.-Y., Liao, C.-H., & Yuan, S.-M. (2024). Self-Sovereign Identity-Based E-Portfolio Ecosystem. *Applied Sciences*, *14*(22), 10361. https://doi.org/10.3390/app142210361
13. Ren, J., Zhang, J., Ren, Y., & Xu, J. (2025). Blockchain-Based Self-Sovereign Identity Management Mechanism in AIoT Environments. *Electronics*, *14*(19), 3954. https://doi.org/10.3390/electronics14193954
14. Liu, J., Liang, Z., & Lyu, Q. (2024). Empowering Privacy Through Peer-Supervised Self-Sovereign Identity: Integrating Zero-Knowledge Proofs, Blockchain Oversight, and Peer Review Mechanism. *Sensors*, *24*(24), 8136. https://doi.org/10.3390/s24248136
15. Le, H. V. A., Nguyen, Q. D. N., Tadashi, N., & Tran, T. H. (2025). Blockchain-Based Decentralized Identity Management System with AI and Merkle Trees. *Computers*, *14*(7), 289. https://doi.org/10.3390/computers14070289
16. Kontzinos, C., Karakolis, E., Kokkinakos, P., Skalidakis, S., Askounis, D., & Psarras, J. (2024). Application and Evaluation of a Blockchain-Centric Platform for Smart Badge Accreditation in Higher Education Institutions. *Applied Sciences*, *14*(12), 5191. https://doi.org/10.3390/app14125191

17. Nazari, Z., Vahidi, A. R., & Musilek, P. (2024). Blockchain and Artificial Intelligence Non-Formal Education System (BANFES). *Education Sciences*, *14*(8), 881. https://doi.org/10.3390/educsci14080881
18. Al-Samarai, B., & Morato, J. (2025). A Systematic Literature Review for the Topic of Blockchain Technology and Educational Systems in the Gulf Cooperation Council (GCC). *Applied Sciences*, *15*(5), 2404. https://doi.org/10.3390/app15052404
19. El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M. Y. (2023). *Unlocking the power of blockchain in education: An overview of innovations and outcomes*. Blockchain: Research and Applications, 4(4), 100165. https://doi.org/10.1016/j.bcra.2023.100165
20. Divyajyothi, M. G., Jopate, R., & Albalushi, R. A. A. (2024, October). AI precision for irrigation, crop management, and pest control for sustainable agriculture in Oman. In IOP Conference Series: Earth and Environmental Science (Vol. 1401, No. 1, p. 012005). IOP Publishing.
21. Jopate, R., M G, D., Devika, P., Veena, S., & Watane, H. N. (2024). Integrating IoT and Blockchain for Secure Computer Network.
22. Jopate, R., Pareek, P. K., & Al Hasani, A. S. Z. J. (2024). Prediction of thyroid classes using feature selection of AEHOA based CNN model for healthy lifestyle. Baghdad Science Journal, 21(5), 29.
23. Divyajyothi, M. G., Jopate, R., Pareek, P. K., & Al Daeri, A. (2025). Water quality prediction and classification using AFSO based long short-term model with data transformation manuscript. Iraqi Journal of Science.
24. Divyajyothi, M. G., & Jopate, R. (2025). Latest Frontiers of Machine, Deep, and Reinforcement Learning Algorithms for Cutting-Edge Applications. In AI Integration for Business Sustainability: For a Resilient Future (pp. 357-371). Singapore: Springer Nature Singapore.
25. Divyajyothi, M. G., Jopate, R., & Lenin, J. (2025). 19 The Future of Trust. Edge AI for Industry 5.0 and Healthcare 5.0 Applications, 269.