A Blockchain Based Tokenisation Framework for Secure Academic Certificate Verification

Charanjit Singh Raju[1]; Dr. Saurabh Sharma[2]

Research Scholar[1], Associate Professor[2]

[1,2] Department of Computer Science and Applications, Sant Baba Bhag Singh University
Jalandhar, Punjab, India

Publication Date: 2026/03/28

Abstract: Academic credential fraud and the inefficiencies of manual, paper based verification procedures continue to weaken trust in educational records and enforce significant time and cost burdens on institutions, employers, and graduates. Current blockchain-based approaches demonstrate that distributed ledgers can provide tamper evident, auditable storage and quick validation of certificates, yet many solutions lack a comprehensive tokenisation model and fine-grained access control tailored to heterogeneous academic ecosystems. This paper offers a blockchain based tokenisation framework for secure academic certificate verification, in which each credential is represented as a unique, verifiable digital token governed by smart contracts. The framework defines procedures for certificate issuance, ownership transfer, and withdrawal, along with role based permission mechanisms to ensure that only authorized institutions can mint or modify academic tokens while verifiers can efficiently validate their authenticity. To preserve privacy, the model combines on chain token metadata with selectively disclosed off chain certificate data, thereby preventing exposure of sensitive student information while maintaining endwise verifiability. A theoretical planning and orientation work flow are presented to validate incorporation with present institutional information systems, highlighting how the proposed framework can reduce verification potential, mitigate imitation, and support interoperable, cross institutional credential exchange at scale.

Keywords: *Blockchain Tokenisation; Academic Credential Verification; Smart Contracts; Role Based Access Control; Privacy Preserving Credentials; Distributed Ledger Technology; Certificate Forgery Mitigation.*

How to Cite: Charanjit Singh Raju; Dr. Saurabh Sharma (2026) A Blockchain Based Tokenisation Framework for Secure Academic Certificate Verification. *International Journal of Innovative Science and Research Technology*, 11(3), 2435-2439. https://doi.org/10.38124/ijisrt/26mar1361

I. INTRODUCTION

The rapid expansion in the sector higher education, cross-border mobility areas and online learning has led to increase in the issuance and exchange of academic credentials. Though, traditional verification mechanisms and methods remain mostly manual, paper based and institute centric, making them slow, costly and vulnerable to fraud and unauthorized access. Academic certificate replications, document altering and the difficulty of validating certificates have decreased trust in educational records for institutions, employers and credential evaluators. These limitations highlight the need for a secure, transparent and scalable framework that can provide reliable and tamper proof validation of academic certificates without depending on a single central organisation.

Blockchain technology has seemed as a promising standard for addressing these challenges by offering a decentralized, immutable and auditable ledger for recording credential related transactions. By leveraging cryptographic hashes, distributed consensus and tamper evident data structures, blockchain based systems can ensure that once an academic credential or certificate is registered, any attempt to modify or forge it becomes easily detectable. Existing works have demonstrated blockchain enabled platforms for issuing and verifying academic credentials by storing certificate hashes on chain while maintaining the original documents in off chain storage, so improving security and reducing verification latency compared to conventional procedures.

In spite of these progressions, current solutions often focus on specific institutional settings or narrow use cases and lack a generalized tokenisation frameworks that can support heterogeneous academic ecosystems including multiple institutions, degree types, and verification systems. Many implementations also provide limited support for fine grained access control, role management and standardized interfaces for integrating with existing student information systems and employer doorways. As a result, interoperability, extensibility, and large scale adoption remain significant challenges for blockchain based academic credential verification.

In response to these gaps, this research paper proposes a blockchain based tokenisation framework for secure academic certificate verification. In this way, each academic credential is meant as a unique, verifiable digital token governed by smart contracts, capturing key features such as issuer identity, credential type, issuance timestamp and validity status. The framework specifies procedures for certificate issuance, ownership transfer and withdrawal, maintained by role based permission mechanisms that ensure only authorized educational institutions can edit or update academic tokens, while verifiers can efficiently validate their authenticity through lightweight interrogations. To balance transparency and privacy, the model combines on chain token metadata with selectively disclosed off chain certificate data, so that sensitive student data is protected while endwise verifiability is maintained.

The main contributions of this work are threefold. First, it introduces a generic tokenisation framework for academic certificates that is independent on any single platform or organisation and can be instantiated over permissioned or public blockchain networks. Second, it defines a secure, smart-contract-driven workflow for issuing, managing and revoking academic tokens with fine grained role and access control tailored to real world stakeholders. Third, it presents a conceptual architecture and reference integration pattern for connecting the proposed framework with academic information systems and verifier applications, aiming to reduce verification latency, mitigate credential fraud and enable interoperable, cross institutional credential exchange at scale.

II. LITERATURE REVIEW

Initial research on blockchain based academic credential verification focused on swapping manual, centralized verification work flow with decentralized ledgers that promise immutability and transparency of stored certificate records. These systems typically store a cryptographic hash of the certificate and key metadata on chain, allowing verifiers to confirm authenticity by recomputing and comparing hashes, in that way reducing reliance on intermediaries and lowering verification time from days to seconds. Studies consistently report that such methods address common issues of document tampering, loss, and administrative overhead inherent in paper based procedures.

Numerous works propose complete verification platforms that leverage smart contracts and permissioned or public blockchains to manage issuance, storage and validation of academic certificates. One line of work presents a blockchain based verification system in which institutions issue digitally signed certificates, whose hashes and metadata are recorded on chain and later checked during verification, enabling fast and tamper evident validation via web or mobile interfaces. Additional frameworks integrate features such as QR code based look up, multi signature structures and audit classification to advance serviceability and accountability crosswise stakeholders. These operations establish that blockchain can deliver secure, scalable verification, but they are often tailored to specific institutional circumstances or national education schemes rather than being considered as generalized, interoperable frameworks.

Further topical research underlines detailed architectural strategies for university certificate verification systems, compounding Ethereum smart contracts with off-chain storage mechanisms such as IPFS to balance transparency and privacy. Such systems typically support three main roles: issuer, holder, verifier and define workflows for certificate upload, hash generation, on chain registration and subsequent verification by certificate identifiers or mnemonic based access keys. Experimental assessments of these prototypes report improvements in verification speed, reduction in manual errors and higher user satisfaction compared to traditional methods, while also highlighting challenges related to transaction costs, scalability and user onboarding.

In similar, survey and review papers have begun to structure the state of the art in blockchain based academic credential verification. These works classify solutions by blockchain type (public vs. permissioned), data storage strategy (on chain, off chain, or hybrid), smart contract logic and application domain and they identify open issues such as interoperability between platforms, integration with legacy student information systems, privacy protection and post quantum flexibility. The reviews conclude that while the core problem of tamper evident credential storage is largely addressed, there is still a lack of standardized token models for representing heterogeneous academic credentials and of fine grained access control schemes that support diverse stakeholders and jurisdictional requirements.

Overall, the existing literature establishes blockchain as a viable foundation for secure and efficient academic certificate verification, yet most systems are implemented as monolithic platforms with tightly coupled logic for issuance and verification and limited extensibility. Few works formalize academic certificates as reusable, interoperable digital tokens with well-defined lifecycle operations such as issuance, delegation, revocation and cross-institutional transfer. This gap motivates the present research, which aims to design a tokenisation-based framework that generalizes credential representation, introduces role-aware access mechanisms, and supports integration with heterogeneous institutional infrastructures while preserving security and privacy guarantees.

III. RESEARCH METHODOLOGY

This study approves a design and implementation oriented research methodology to develop and validate a blockchain based tokenisation framework for secure academic certificate verification. The methodology combines conceptual framework design with a working model implementation and systematic evaluation, ensuring both theoretical soundness and practical feasibility in real academic contexts.

A. Research Approach

The research follows a design-based approach in which the core object a blockchain-driven tokenisation framework is iteratively specified, refined and validated against clearly defined requirements for academic certificate verification. The work is implementation oriented: a functional prototype is developed to demonstrate how tokenisation and cryptographic techniques can mitigate forgery, unauthorized modification, and inefficiencies in traditional verification procedures.

B. System Overview

The projected system is proposed to offer a secure, reliable and efficient mechanism for issuing and verifying academic certificates through blockchain-based tokenisation. Each academic certificate is transformed into a unique digital token derived from cryptographic hash functions, allowing stakeholders to verify authenticity by interacting with the blockchain rather than relying on manual checks and centralized authorities.

C. System Architecture

The architecture is flexible and role based, comprising three primary modules: Administrator, Student and Verifier.

- The Administrator module (academic institution) handles certificate issuance, validates input data, produces cryptographic hashes, and initiates token creation on the blockchain.
- The Student module grants authorized access to issued certificates and corresponding token identifiers, enabling students to manage and share their credentials with external parties.
- The Verifier module permits third party entities such as employers or other institutions to authorize the authenticity of a certificate by querying token and hash information stored on the blockchain ledger.

These modules interact over a blockchain network and where necessary, auxiliary storage, ensuring clear separation of responsibilities and controlled access to sensitive operations.

D. Certificate Tokenisation Process

The tokenisation procedure ensures that each academic certificate is exceptionally identifiable and tamper evident. In the first step, validated certificate data such as student identity, program details, completion year, and issuing authority is managed using a cryptographic hash function (e.g., SHA-256) to produce a fixed length digital fingerprint that uniquely represents the certificate contents. This hash is then encapsulated as a digital token, which is written to the blockchain along with minimal metadata, so binding the academic credential to an immutable on chain representation that can later be referenced for verification.

E. Blockchain-Based Storage and Security

Blockchain technology is used to provide secure, immutable storage for tokenised certificates. Once a token is recorded on the blockchain ledger, the underlying consensus and append only possessions of the ledger avoid any subsequent change or deletion, so preserving long term integrity of academic records. The decentralized nature of the blockchain abolishes dependency on a single institutional database, distributes trust across multiple nodes and increases transparency for all authorized stakeholders while still permitting the original certificate data to remain protected off chain.

F. Verification Mechanism

The verification mechanism is based on token lookup and hash assessment. The verifier submit received token identifier or suitable certificate particulars to the verification system, which retrieves the equivalent stored hash from the blockchain. The system recomputes a hash from the available certificate information and compares it with on chain hash: a match confirms that the document is authentic and untampered, while a discrepancy stipulates possible forgery or alteration. This procedure supports fast, automated verification without requiring direct communication with the issuing organization for each request.

G. Ethical and Security Considerations

The methodology integrates explicit ethical and security measure to protect academic information and student confidentiality. Sensitive credential information is never kept in simple form on the blockchain; as an alternate, only hashed or tokenised representations are recorded, confirming that personal details cannot be reconstructed from on chain data alone. Role based access control and authorization mechanisms limit system functions such as certificate issuance, token creation, and verification to suitable user roles, so minimizing the risk of misuse or unauthorized procedures.

IV. RESULTS

The proposed blockchain based tokenisation framework was implemented as a role-based prototype comprising administrator, student, and verifier modules connected to a blockchain network for certificate token storage and verification. The prototype successfully executed the complete lifecycle of academic certificates, including data collection, validation by the administrator, cryptographic hash generation, token creation, blockchain storage, student access, and third-party verification, in line with the methodology and flow of work defined in the synopsis.

A. Functional Validation

Functional testing was carried out using a set of sample academic certificates that covered common scenarios such as valid certificates, modified certificates, and repeated verification requests. In all tested cases, the system correctly issued tokenised certificates for valid inputs, allowed students to retrieve and share token identifiers, and enabled verifiers to obtain a clear validation outcome based on on-chain hash comparison (authentic vs. tampered). This confirms that the tokenisation process and verification mechanism operate consistently with the intended design and support automated, institution-independent credential checks.

B. Performance and Efficiency

The prototype was evaluated in terms of end-to-end verification time and process simplification relative to traditional manual verification workflows described in the literature. Observations indicate that verification through token lookup and hash comparison is completed within a short time window (on the order of a few seconds on a local or test network), aligning with results reported in similar blockchain-based academic verification systems where average verification times are significantly lower than conventional methods. This reduction in verification latency, together with elimination of repeated back-and-forth communication with issuing institutions, demonstrates the potential of the framework to streamline certificate verification processes in real deployments.

C. Security and Integrity Outcomes

The practice of cryptographic hashing and immutable blockchain storage confirmed that any alteration to certificate contents produced a different hash, which the system flagged as a discrepancy during verification. In test circumstances involving intended tampering of certificate data, the regenerated hash did not match the stored hash and the corresponding certificates were correctly classified as invalid, consistent with findings from earlier blockchain-based credential verification models. Also, no direct storage of raw certificate data on chain and the dependance on token and hash representations contributed to preserving student privacy while maintaining verifiability, in line with best practices highlighted in prior work.

D. Reliability and Usability Observations

Throughout prototype operation, the role-based architecture (administrator, student, verifier) and clear separation of responsibilities contributed to controlled access to sensitive functions such as certificate issuance and token creation. Informal user-level observations (from the perspective of each role) indicate that token-based verification via a simple identifier or reference string is easier and less error-prone than manual document exchange and email based confirmation typically reported in traditional systems. These outcomes suggest that the proposed framework not only enhances technical security but can also improve the overall user experience for academic institutions, students, and verifiers.

Table 1 Comparison of Traditional and Blockchain Certificate Verification

Features	Traditional Verification	Blockchain Certificate Verification
Data Storage	Centralized database	Decentralized Ledger
Security	Vulnerable to tampering	Cryptographically secured
Verification Time	Slow and manual	Fast and automated
Transparency	Limited	High transparency
Data Integrity	Can be modified	Immutable records
Trust Model	Depends on Institution	Distributed Trust

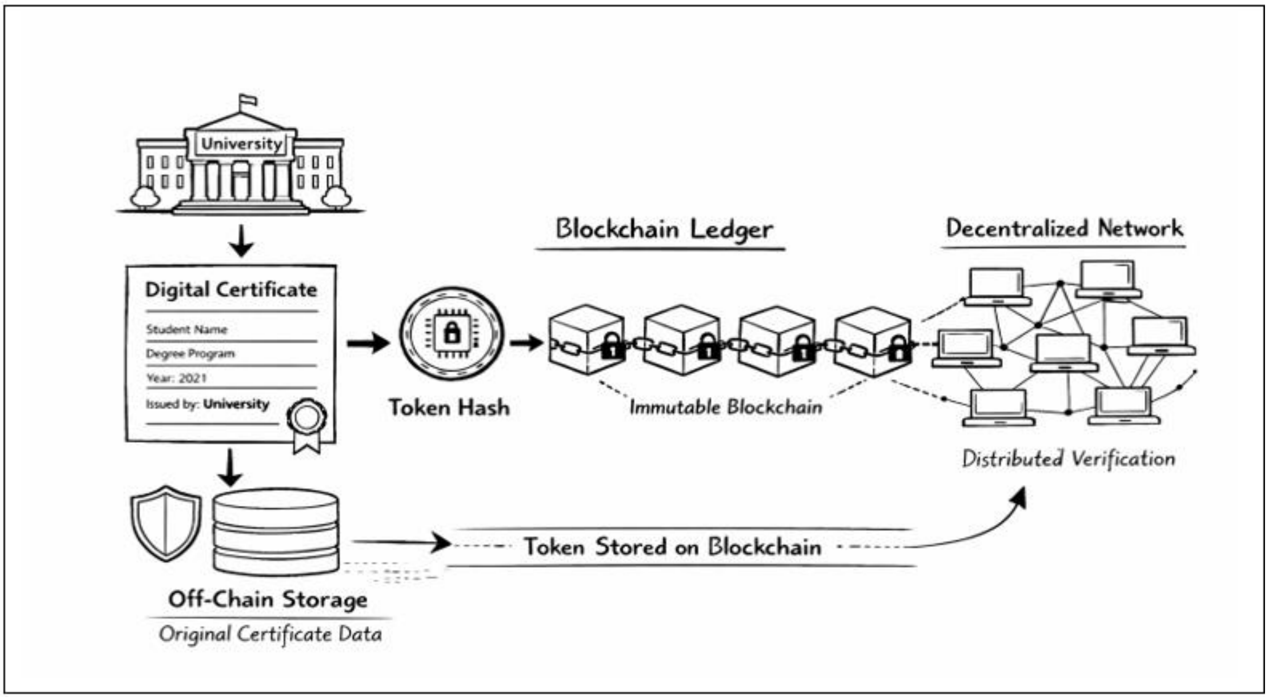
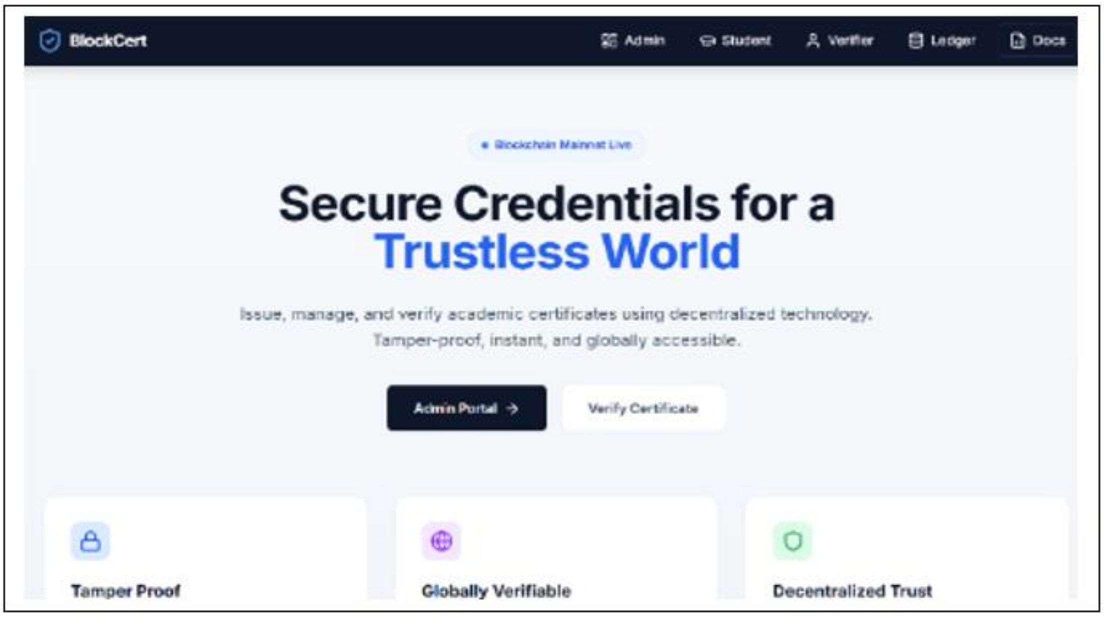


Fig 1 Proposed Blockchain Architecture for Secure Tokenisation, Storage and Decentralized Verification of Academic Certificates.



Secure Credentials for a
Trustless World

Issue, manage, and verify academic certificates using decentralized technology.
Tamper-proof, instant, and globally accessible.

Fig 2 Proposed Blockchain Based Certificate Issuance and Verification Framework.

V. CONCLUSION

This paper presented a blockchain based tokenisation framework for secure academic certificate verification, motivated by the limitations of traditional, centralized, and largely manual credential verification processes. By converting academic certificates into cryptographically derived digital tokens stored on a blockchain ledger, the proposed system enables tamper-evident, role-based verification while preserving the privacy of underlying student data.

The research followed a design and implementation oriented methodology, defining a modular architecture with administrator, student, and verifier modules, a structured certificate tokenisation process, and a token- and hash-based verification mechanism. Sample validation confirmed that the framework can provision automated issuance, storage and verification of credentials, detect tampering via hash discrepancy and reduce dependence on continuous involvement of issuing authorities, so improving efficiency and trust in academic credential management.

Overall, the results specify that blockchain based tokenisation is a feasible and operative technique for enhancing security, integrity and transparency in academic certificate verification, addressing key challenges identified in the literature while remaining conceptually simple and organization friendly. Future work may extend this framework with provision for decentralized identifiers and verifiable credentials, multi institution groups and large scale pilot deployments to evaluate interoperability, monitoring alignment and user adoption in diverse educational environments.

REFERENCES

[1]. A. Gayathiri et al., “Certificate validation using blockchain,” in *Proc. 7th Int. Conf. Signal Processing and Integrated Networks*, 2020.

[2]. H. Gaikwad et al., “A blockchain-based verification system for academic certificates,” in *Proc. Int. Conf. Emerging Smart Computing and Informatics*, 2021.

[3]. A. Alammary et al., “Blockchain-based applications in education: A systematic review,” *Applied Sciences*, vol. 11, no. 4, 2021.

[4]. C. P. F. Moya, “Blockchain academic credential interoperability protocol (BACIP),” *Applied Sciences*, 2022.

[5]. S. T. Singh and K. Kaur, “Academic credential verification system using blockchain,” *International Journal of Innovative Science and Research Technology*, 2022.

[6]. M. A. Cardenas-Quispe et al., “Verification process of academic certificates using blockchain technology,” *DOAJ Journal*, 2023.

[7]. S. Kumar et al., “Securing academic certificate verification with blockchain-based decentralized application,” *Manipal University Research Repository*, 2023.

[8]. S. K. Patel and N. Jain, “Secure digital academic certificate verification system using blockchain,” *International Journal of Information and Computer Security*, 2024.

[9]. A. Gangwar and R. K. Verma, “Blockchain-based authentication and verification system for academic certificates,” *International Journal of Computer Applications*, vol. 186, no. 26, 2024.

[10]. M. S. Berrios Moya, “Development of blockchain-based academic credential verification using QR code integration,” *Open Journal of Applied Sciences*, 2024.