STM JOURNALS

Journal of
Computer Technology & Applications

ISSN: 2229-6964 (Online)
ISSN: 2347-7229 (Print)
Volume 17, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoCTA

https://journals.stmjournals.com/jocta

Review JoCTA

Enhancing Trust in Education Through Blockchain-Based Credential Authentication

Nirav K. Shah[1,*], Arpit B. Parekh[2]

Abstract

Academic credentials such as degree certificates, transcripts, and course completion records are fundamental for validating an individual's educational achievements. However, conventional credential management systems largely rely on centralized databases and physical documentation, making them vulnerable to forgery, unauthorized modification, data loss, and inefficient verification processes. These limitations reduce trust among educational institutions, employers, and learners, while also increasing administrative overhead. This study proposes a blockchain-based credential authentication framework designed to enhance trust, transparency, and security within the education ecosystem. The proposed system leverages a permissioned blockchain network to record immutable digital fingerprints of academic credentials, while the original documents are securely stored in encrypted off-chain repositories. Smart contracts are employed to automate credential issuance, validation, and revocation, ensuring consistency and eliminating manual intervention. Students are provided with controlled access to their academic records, enabling secure and selective sharing with authorized verifiers such as employers or higher education institutions. A prototype implementation demonstrates that the proposed approach significantly reduces credential verification time while ensuring data integrity and tamper resistance. The hybrid on-chain and off-chain storage model effectively balances security requirements with scalability and storage efficiency. The findings indicate that blockchain technology can address critical challenges associated with traditional academic credentialing systems and offers a reliable foundation for future digital credential management. The proposed framework has strong potential for adoption across educational institutions seeking secure, transparent, and efficient credential authentication mechanisms.

Keywords: Blockchain, credential authentication, digital verification, education technology, smart contracts

INTRODUCTION

Academic credentialing is a critical function of educational institutions, serving as formal proof of a learner's knowledge, skills, and academic accomplishments. Degrees, diplomas, certificates, and transcripts are widely used for higher education admission, employment screening, professional licensing, and international mobility. As educational systems expand globally and learner mobility increases, the demand for reliable, secure, and easily verifiable academic credentials has grown significantly. However, traditional credential management systems have struggled to meet these evolving requirements.

Most existing academic record systems rely on centralized databases, paper-based certificates, or institution-specific digital repositories. Although

***Author for Correspondence**
Nirav K. Shah
E-mail: nkshah.mca@gmail.com

[1]Assistant Professor, Shree Swaminarayan College of Computer Science, M.K. Bhavnagar University, Bhavnagar, Gujarat, India
[2]Assistant Professor, Shree Swaminarayan College of Computer Science, M.K. Bhavnagar University, Bhavnagar, Gujarat, India

Received Date: December 16, 2025
Accepted Date: December 21, 2025
Published Date: February 03, 2026

Citation: Nirav K. Shah, Arpit B. Parekh. Enhancing Trust in Education Through Blockchain-Based Credential Authentication. Journal of Computer Technology & Applications. 2026; 17(1): 1–7p.

these approaches have served institutions for decades, they present several inherent weaknesses. Centralized storage systems create single points of failure, making records vulnerable to cyberattacks, accidental data loss, and system outages. Paper certificates can be easily forged, altered, or duplicated, whereas digital documents stored without strong cryptographic protection are susceptible to manipulation. Consequently, trust in academic credentials can be compromised, leading to serious consequences for institutions, employers, and learners.

Credential verification is another major challenge for traditional systems. Employers and academic institutions often need to manually contact the issuing authorities to confirm the authenticity of certificates. This process is time-consuming, costly, and inefficient, particularly when verification involves international institutions or records. Students and alumni may also face difficulties in accessing their credentials years after graduation, especially if institutions merge, close, or migrate to new systems. These inefficiencies highlight the need for more resilient and transparent credentialing mechanisms [1].

Blockchain technology has emerged as a promising solution for addressing trust-related challenges across various domains, including finance, supply chain management, healthcare, and governance. Its core characteristics, decentralization, immutability, transparency, and cryptographic security, make it well-suited for applications where data integrity and trust are paramount. Once data are recorded and validated in a blockchain network, they cannot be altered without consensus from authorized participants, ensuring a tamper-resistant record of transactions [2].

Applying blockchain technology to academic credentials has introduced a paradigm shift in how educational records are issued, stored, and verified. Instead of relying on centralized authorities, credentials can be recorded on a distributed ledger shared among trusted institutions. Each credential is represented by a cryptographic hash that ensures authenticity without exposing sensitive personal data. Smart contracts further automate the credential lifecycle, enabling secure issuance, verification, and revocation, with minimal human intervention [3].

In addition to enhancing security, blockchain-based credentialing systems empower students by providing them with greater control over their academic data. Learners can securely share verifiable credentials with employers or institutions, without relying on intermediaries. This model supports privacy-preserving verification while maintaining transparency and trust. Furthermore, hybrid architectures that combine on-chain verification with off-chain document storage address the scalability and storage limitations of blockchain systems [4].

This study explores the design and implementation of a blockchain-based credential authentication framework tailored for educational institutions. The proposed system aims to strengthen trust in academic records by ensuring data integrity, improving verification efficiency, and reducing fraud risk. By leveraging permissioned blockchain technology and smart contracts, this framework provides a practical and scalable solution for modern academic credentials.

PROBLEM STATEMENT

Despite advancements in digital record management, traditional academic credentialing systems continue to face critical challenges that undermine trust, efficiency, and security. The challenges are outlined as follows:

Credential Forgery and Fraud

The increasing availability of advanced printing and digital editing tools has facilitated the creation of counterfeit certificates and the manipulation of academic records. Fake degrees and altered transcripts pose a serious risk to employers, educational institutions, and regulatory bodies. Existing systems often lack effective mechanisms for detecting tampering, allowing fraudulent credentials to circulate undetected.

Centralized System Vulnerabilities

Most academic records are stored in centralized databases managed by individual institutions. Such systems are vulnerable to cyberattacks, unauthorized access, hardware failures, and natural disasters. A single system failure can result in a permanent loss or compromise of critical academic data [5].

Inefficient Verification Processes

Credential verification typically involves manual communication between verifying and issuing organizations. This process is slow, resource-intensive, and prone to delays, particularly for international verification requests [6]. The lack of standardized verification mechanisms further complicates cross-institution and cross-border credential validation.

Limited Student Control and Transparency

Students often have little control over how their academic records are stored, accessed, or shared. They must rely on institutions to issue transcripts or confirm credentials, which can be inconvenient and costly [7]. Additionally, students have limited visibility in accessing their data and for what purpose.

Scalability and Interoperability Issues

Existing credential systems are typically designed for individual institutions and lack interoperability with other academic and professional platforms. This fragmentation limits scalability and prevents the creation of unified credential verification networks at the regional, national, or global levels [8].

Trust Deficit in Digital Credentials

Without a universally trusted verification mechanism, digital credentials are often viewed with skepticism. Institutions and employers require assurance that digital records are authentic, untampered with, and issued by legitimate authorities [9].

Problem Definition

There is a clear need for a secure, tamper-proof, transparent, and efficient authentication system for academic credentials.

- Prevents credential forgery and unauthorized modification
- Eliminates reliance on centralized storage
- Enables instant and reliable verification
- Preserves student privacy and data ownership
- Supports interoperability across institutions

Blockchain technology offers a viable foundation to address these challenges by providing immutable records, decentralized trust, and automated verification mechanisms.

Objectives

The main objectives of this research are:

1. To design a blockchain-based system for secure academic credential authentication.
2. To prevent forgery by making academic records immutable and verifiable.
3. To simplify credential verification for employers and institutions.
4. To enhance transparency while preserving student privacy.
5. To provide a hybrid on-/off-chain model to balance security and storage efficiency.

LITERATURE REVIEW

The growing demand for secure and verifiable digital credentials has motivated extensive research into blockchain-based solutions in the education sector [10]. This section reviews recent and relevant studies published between 2021 and 2025, focusing on blockchain adoption for academic credential management, digital identity, and verification systems [11].

Blockchain in Educational Record Management

Recent studies have emphasized the suitability of blockchain technology for managing educational records because of its decentralized and immutable nature. Researchers have highlighted that blockchain can address long-standing issues of trust and data integrity in academic systems by ensuring that once a credential is recorded, it cannot be altered or deleted without authorization. Permissioned blockchain networks have been particularly recommended for educational use, as they allow institutions to retain governance control while benefiting from decentralization.

Several works have proposed blockchain-based academic record repositories that replace centralized databases with distributed ledgers shared among trusted institutions. These systems reduce dependency on a single authority and improve resilience against cyber threats and system failure. However, researchers also note that the purely on-chain storage of academic documents is impractical because of scalability and cost concerns [2].

Digital Credentials and Verification Challenges

Digital credential verification remains a complex challenge, particularly in cross-institutional and international contexts. Recent literature highlights that manual verification processes are inefficient and prone to delays, which negatively impact student mobility and employment opportunities. Blockchain-enabled verification systems offer automated validation through cryptographic proofs, significantly reducing verification time and administrative workload.

Studies conducted after 2021 demonstrate that blockchain-based credentials can be verified independently by employers without direct communication with issuing institutions. This capability improves trust while reducing operational costs. However, researchers have emphasized the importance of standardization to ensure interoperability across blockchain platforms and educational systems.

Smart Contracts for Credential Lifecycle Management

Smart contracts have been widely explored as mechanisms for automating credential-related processes. Recent research shows that smart contracts can enforce predefined rules for credential issuance, verification, and revocation, ensuring consistency and reducing human error. By embedding institutional policies directly into blockchain, smart contracts enable transparent and auditable credentials.

Several studies have also highlighted the role of smart contracts in handling credential revocation, which is often overlooked in traditional systems. Revocation mechanisms are essential to address errors, disciplinary actions, and credentials. Blockchain-based revocation records ensure that verifiers always access current credentials.

Privacy and Security Considerations

Privacy preservation is a major concern in blockchain-based educational systems. Recent literature stresses that storing personal data directly on the blockchain can conflict with data-protection regulations. To address this issue, researchers have proposed a hybrid architecture that stores sensitive documents off-chain, while recording cryptographic hashes on-chain [3].

Advanced techniques, such as encryption, access control, and selective disclosure, have been explored to protect student data. Some studies have also investigated the use of zero-knowledge proofs to enable verification without revealing underlying data. These approaches demonstrate that blockchain systems can achieve transparency and privacy when appropriately designed.

Existing Platforms and Limitations

Several blockchain-based credentialing platforms and pilot projects have been reported in the recent literature. These implementations demonstrate the practical feasibility of blockchain technology in academic credentials. However, the limitations related to scalability, governance, interoperability, and user adoption remain significant challenges.

Researchers emphasize that many existing solutions are either platform-specific or lack flexibility for regional or national deployment. There is a clear need for adaptable frameworks that can be integrated into existing institutional systems while supporting future expansion.

Research Gap

While prior studies confirm the potential of blockchain for academic credentials, gaps remain in terms of the following:

- Practical deployment models for permissioned educational networks
- Efficient hybrid storage architecture
- Student-centric access control mechanisms
- Comprehensive evaluation of system performance

This study addresses these gaps by proposing a scalable, permissioned blockchain-based credential authentication framework with hybrid storage and automated verification capabilities.

PROPOSED SYSTEM ARCHITECTURE

The proposed model is based on a permissioned blockchain network that includes universities, colleges, accreditation bodies, and authorized verifiers as nodes.

Key Components

- *Blockchain network*: Stores cryptographic hashes of credentials and smart contract operations.
- *Smart Contracts:*
  - Issue new credentials
  - Validate credentials
  - Revoke or update records
- *Off-chain storage InterPlanetary File System (IPFS) cloud:* Stores actual documents in encrypted form.
- *Student wallet:* Mobile or web-based applications where students store access keys and share credentials.
- *Verifier portal:* Employers or institutions can verify documents instantly by checking blockchain records.

Workflow

1. The institution generates a student certificate or transcript.
2. Document is encrypted and stored off-chain.
3. The hash of the document, along with the metadata are stored in the blockchain via a smart contract.
4. Students receive a unique credential ID or Quick Response (QR) code.
5. A verifier scans the code, retrieves the document, computes its hash, and compares it with the blockchain entry.
6. If the hashes match, the credential is verified as authentic.

Data Model

On-Chain Data

- Credential ID
- Issuer ID
- Recipient ID (hashed)
- Document hash
- Issue date
- Credential status (active/revoked)

Off-Chain Data

- Full certificate or transcript
- Encryption keys
- Access control settings

This separation ensures both privacy and efficiency.

IMPLEMENTATION DETAILS

A prototype was implemented using:

- *Hyperledger fabric*: as the permissioned blockchain
- *Node.js smart contracts*: to manage credential lifecycle
- *InterPlanetary File System (IPFS)*: for off-chain encrypted storage
- *React-based user interfaces*: for issuers, students, and verifiers

The initial testing involved creating sample student records and simulating verification requests. The system demonstrated fast lookup and verification with minimal computation.

RESULTS AND DISCUSSION

The prototype produced several promising results:

- *Verification time has been reduced significantly* compared to manual processes.
- *Tamper detection* became immediate due to hash mismatch alerts.
- *Students gained more control* over how their credentials are shared.
- *Institutions could track all issued records* in an immutable ledger.

However, challenges remain regarding large-scale deployment, cross-institution coordination, and ensuring compatibility with existing digital identity frameworks.

Advantages of the Proposed System

- *Tamper-proof records*: Immutable blockchain entries make forgery extremely difficult.
- *Fast verification:* Employers can verify credentials in seconds.
- *Improved transparency:* Complete audit trails for each credential.
- *Enhanced trust:* Institutions and employers rely on the same decentralized source of truth.
- *Student empowerment:* Learners maintain control over their academic data.

Limitations

- Requires technological infrastructure and training.
- A cross-institution agreement is necessary for network adoption.
- Storing large documents on-chain is not feasible; hence, off-chain dependency remains.
- Blockchain governance policies must be clearly defined.

Future Scope

Several enhancements may be possible in the future:

- Integration with national digital identity systems.
- Use of zero-knowledge proofs for privacy-preserved verification.
- Support for international cross-border credential exchange.
- Fully automated recognition of foreign academic qualifications.
- Deployment in Massive Open Online Courses(MOOCs) and lifelong learning ecosystems.

CONCLUSION

Blockchain provides a strong foundation for improving trust in academic credentials. By combining decentralized storage, cryptographic security, and smart contract automation, educational institutions

can ensure that their academic records remain authentic, verifiable, and tamper-proof. The proposed blockchain-based credential authentication framework demonstrated that trust in education can be significantly enhanced by adopting modern technology. As more institutions recognize the need for secure and transparent record management, blockchain is likely to become a key component of academic administration in the future.

REFERENCES

1. Verma PK, Sharma V, Kumar P, Sharma S, Chaudhary S, Preety P. IoT enabled real time appearance system using AI camera and deep learning for student tracking. Int J Recent Innov Trends Comput Commun. 2023;11:249–254. doi:10.17762/ijritcc.v11i6s.6885.
2. Alammary A, Alhazmi S, Almasri M, Gillani S. Blockchain-based applications in education: A systematic review. Appl Sci. 2019;9(12):2400. doi:10.3390/app9122400.
3. Turkanović M, Hölbl M, Košič K, Heričko M, Kamišalić A. EduCTX: A blockchain-based higher education credit platform. IEEE Access. 2018;6:5112–5127. doi:10.1109/ACCESS.2018.2789929.
4. Rawat DB, Chaudhary V, Doku R. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. J Cybersecur Priv. 2020;1(1):4–18. doi:10.3390/jcp1010002.
5. Al Mamun AA, Azam S, Gritti C. Blockchain-based electronic health records management: A comprehensive review and future research direction. IEEE Access. 2022;10:5768–5789. doi:10.1109/ACCESS.2022.3141079.
6. Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Comput Surv. 2019;52(3):1–34. doi:10.1145/3316481.
7. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Inf Sci. 2015;305:357–383. doi:10.1016/j.ins.2015.01.025.
8. Cai W, Wang Z, Ernst JB, Hong Z, Feng C, Leung VCM. Decentralized applications: The blockchain-empowered software system. IEEE Access. 2018;6:53019–53033. doi:10.1109/ACCESS.2018.2870644.
9. Alam S, Ayoub HAY, Alshaikh RAA, AL-Hayawi AH. A blockchain-based framework for secure educational credentials. Turk J Comput Math Educ. 2021;12(10):5157–5167. doi:10.17762/turcomat.v12i10.5298.
10. Dwivedi AD, Srivastava G, Dhar S, Singh R.A decentralized privacy-preserving healthcare blockchain for IoT. Sensors. 2019;19(2):326. doi:10.3390/s19020326.
11. Chen G, Xu B, Lu M, Chen NS. Exploring blockchain technology and its potential applications for education. Smart Learn Environ. 2018;5(1):1–10. doi:10.1186/s40561-017-0050-x.

