Publisher homepage: www.universepg.com, eISSN: 2663-7804

Australian Journal of Engineering and Innovative Technology

Journal homepage: www.universepg.com/journal/ajeit

OPEN ACCESS | Research Article

Blockchain Technology for Academic Credential Verification Preventing Transcript Fraud in the USA

Sathy Akter*

Master of Instructional Technology, Touro University of New York, Manhattan, NY, United States of America

*Correspondence: sornallysathy2017@gmail.com (Sathy Akter, Master of Instructional Technology, Touro University of New York, Manhattan, NY, United States of America).

Received Date: 7 July 2026 Accepted Date: 5 August 2026 Published Date: 12 August 2026

Abstract

Currently, the most significant threat to the validity of academic credentials in the United States is the advanced forgery of transcripts along with diploma mills. This research study addresses the potential of blockchain technology as a decentralized means to protect academic credentials. By integrating recent academic research and technical frameworks, this study analyzes the shift from centralized databases to immutable, distributed ledgers. The integration of various perspectives, including advanced zero-knowledge proof architectures as well as legal frameworks for transnational data circulation, is a major innovation of this study. Using a systematic literature review and a case study approach, the research indicates that though blockchain's potential to enhance security and automate processes through smart contracts is indeed great, a number of legal, compliance, and technical barriers have to be removed for it to be a viable option. This study proposes that the combination of artificial intelligence (AI), along with blockchain technology, provides the most secure option for U.S. higher education institutions.

Keywords: Blockchain technology, Academic credentials, Smart contracts, Higher education, Sovereign identity.

1. Introduction

Research Problem

The normal systems to oversee academic records in the United States has become badly outdated. Previously, the Centralized University Databases were adequately functional, but at present, they are more likely to fail due to both external and internal risks. Digitally changing transcripts has led to an emergent crisis of faith in the job market. Unions and certification boards must depend on time-consuming manual checks, which cannot guarantee authenticity. The combination of worldwide academic scams and advanced hostile A.I. creates a demand for a system to create confidence in the results of education and provide verification that cannot be altered.

Purpose of the Study

This study examines whether blockchain technology could help combat transcript fraud in the U.S. education system. This study attempts to evaluate whether a decentralized system can address the issue of confidential student information and the necessity of institutional autonomy while retaining a verified single source of truth concerning student achievements. The study also aims to investigate the shift

from paper and/or digitally disconnected systems to a fully integrated, decentralized system, as well as the U.S. education system's readiness for this shift.

Research Objectives and Hypotheses

The research objectives and related hypotheses are outlined below:

1) To assess the advantage of blockchain-based verification systems over existing central systems that dominates the U.S. higher education system.
2) To assess the possibility of reduced administrative errors using smart contracts in conjunction with the automation of both the enrollment process and the issuance of transcripts.
3) To assess the constraints, including legal and technological, of privacy of personal data and the inability of standardized technological interoperability to enable the broad deployment of these systems across the U.S.

The associated hypotheses are outlined below:

The first hypothesis states that the risk of identity theft and credential forgery will be reduced when compared to existing systems, using blockchains that are integrated with zero knowledge proofs.

The second hypothesis states that the technology used by educational institutions to implement blockchain technology is the least of their concerns, and that more of their concerns are of a regulatory and social nature.

Research Questions (RQ)

Three questions provide the main structure to this research work:

RQ1: How far does blockchain decentralization reduce the frailties found in U.S. university Centralized Transcript Management Systems?

RQ2: What improvements do smart contracts and automated processes in the issuance of credentials provide in the prevention of administrative fraud and in the enhancement of the security and efficiency of credential issuance?

RQ3: What are the main legal and technological obstacles to the Unified Cross-Domain Blockchain for Academic Verification in the U.S.?

Significance of Study

The research aims to be beneficial for university registrars, policymakers, and human resource management personnel. Aiming to provide a comparative analysis of current theoretical models and pilot projects, it provides a framework to protect the "brand" of U.S. education. The authors provide a range of materials from 2024 to 2026 to identify the most recent changes in the dynamic fields (in the intersection of blockchain with Artificial Intelligence and Internet of Things), providing insight to the U.S.-based institutions on standards required to retain postgraduate competitiveness and how they can retain competitiveness in a global area using secure and seamless credential exchange.

Concepts and Critical Definitions

Blockchain is a type of distributed ledger technology that uses cryptographic hashing to create a record of transactions in a way that is spread across numerous nodes in a way that is immutable. Smart contracts are a type of contract that is executed by a computing solution, without the need for further human intervention, by satisfying pre-defined conditions, such as the release of a person's degree when they have completed the requirements for that degree. Transcript fraud is the illegal alteration, creation, or misrepresentation of an individual's academic record. Zero-knowledge proofs (ZKPs) are methods of cryptography where one individual can validate or prove that a particular statement is true to another individual, without revealing or disclosing that statement. This can be relevant in maintaining compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA) in the United States, as it is one of the primary concerns in the implementation of blockchain and ZKPs.

Assumptions, Limitations, and Delimitations

Assumptions

It is assumed that, in the United States, there will be continued digitization of records by the greater sector of higher education, and that there is a concern from the greater sector of higher education to reduce the costs and impact of record verification and academic fraud. It is also assumed that the technologies cited in the literature, such as smart contracts on the Ethereum

blockchain, or the Hyperledger frameworks, are at a level of sufficient scale to accommodate the higher education system in the United States.

Limitations and Delimitations

The primary limitation is the unavailability of long-term longitudinal studies for the implementation of blockchain technology, as most use cases are still in the pilot's stage. The study is delimited to the higher education sector in the United States, but its focus is on international benchmarking from the Gulf Cooperation Council (GCC) and the European Union (EU). It does not focus on the financial records and the athletic records of students. The primary focus of the study is on academic transcripts.

2. Review of Literature

Theoretical Framework: Decentralization and Trust

This research is anchored on the transition from institutional trust to algorithmic trust. Chen *et al.* (2018) were the first to assess the potential of blockchain for education by decentralizing and moving away from a single institution as the authoritative body for the truth. This idea aligns with the concept of the "lifelong learning passport" as proposed by Gräther *et al.* (2018), which places the learner at the center of the credentialing system rather than the institution. This is especially necessary within the U.S. context where the institutional silos hinder the movement of records from one institution to another. Fleener, (2022) adds to this by stating that the future of education relies on the technologies becoming "invisible" through the integration of the trust as a feature of the system.

Technical Architectures for Credential Security

Berrios Moya *et al.* (2025) inspect the workings of security and provide an example of a system with an embedded zero-knowledge proof, which answers a concern of publicly available blockchains privacy. With verification possible without data being revealed, the model proposed does solve the problem between the tension of transparency and FERPA compliance in the USA. This model of a technical solution is in contrast to the broader systematic review of Al-Samarai and Morato, (2025) where, in the Gulf Cooperation Council (GCC) Literature, U.S.-centered Literature that they review, as cited by Sharwani and Melo, (2024) focuses on the prevention of specific types of frauds (e.g., diploma mills). The comparison of the regions indicates that the implementation of methods is influenced by the systems of governance in a region, although the technical solutions might be similar. There is an increasing significance of the combination of hardware security and decentralized access. Na and Park, (2022) discuss a type of "IoT-chain" architecture, which implies that the classroom sensors that record grades and attendance may be secure chain nodes. This idea of multilevel security is supported by Usama *et al.* (2026) who argue that to protect identity management systems from deepfake academic and other records, an adequate defense in depth must be deployed against category adversarial AI attacks. According to Sun *et al.* (2021), something similar can be said for lightweight access control systems provided in mobile-based secure blockchain systems in education. In order for the blockchain not to become a point of failure, and to ensure that legitimate users are not obstructed, lightweight access control systems are provided (Sokhandan, 2024).

Smart Contracts and Administrative Automation

Smart contracts are the functional element of this shift in technology. James, (2025) provides an in-depth analysis of contracts that can automate the enrollment of students, collection of fees, and management of student transcripts in an effort to reduce human involvement in these processes to eliminate (or at least reduce) the opportunity for fraudulent manipulation. Patel and Das, (2019) illustrate that smart contracts can manage a transcript from the first credit completed to the last award of a degree. Fedorova and Skobleva, (2020) believe that this represents an improvement of the process. Automation, if sufficient care is taken to ensure the data is entered correctly, creates an audit trail that is, cryptographically speaking, unalterable. The literature indicates that the real breakthrough in limiting the consequences of internal administrative malfeasance stems from the transition to the automated issuance of documents.

Legal and Regulatory Landscape

Legally, the storage of academic data on a distributed ledger is a collection of challenges. Walters and Takman, (2026) describe the complications of cross

border flows of personal data. As students from the US migrate internationally, the blockchain records of these students must comply with the laws of these countries. This is exemplified when comparing the USA with the European setting described in Camilleri, (2017) and in Raimundo and Rosário, (2021) where the General Data Protection Regulation (GDPR) sets a stringent requirement for data protection. Delgado von-Eitzen *et al.* (2021) argue that any academic blockchain must be "GDPR-compliant by design" and U.S. regulators will, most likely, must adopt this principle soon to adjust to global standards. The conflict of the "right to be forgotten" and the "immutability of the chain" is, and will conitinue to be, a topic of legal discourse in 2026.

Comparative Analysis of Adoption and Readiness

The propensity of different groups to adopt these technologies is the central issue. Sovtić *et al.* (2025) discuss readiness from the standpoint of consumer behavior. This can be extended to the university registrars - if the prevention of fraud is deemed a benefit of the inclusion of a new system, then the new system will be adopted. This leans towards the findings of Marnita *et al.* (2025), whose analysis of teacher credentialing describes that change in an organization is brought about by the "transparency and trust" of the stakeholders. In the USA, Alammary *et al.* (2019) provide an extensive analysis of applications, and suggest that their adoption is, often, concentrated in multiple "innovation hubs" and not across the country.

Synthesis: The Emergence of Hybrid Models

Some researchers believe that blockchain may not be enough to tackle modern counterfeiting. Ghadi *et al.* (2025) present a hybrid AI-Blockchain model. Although their case is that of smart grids, the same logic can be applied within the context of education: AI can track fraudulent behaviors (e.g. anomalous grading) in real-time, while blockchain can store an unalterable and permanent record of the case. This combination is aimed at both the real-time detection of fraud and at the verification of authenticity.

Table 1: Comparative Analysis of Credential Verification Models.

Feature	Centralized (Traditional)	Standard Blockchain	Hybrid AI-Blockchain (Proposed)
Trust Source	Institutional Authority	Algorithmic Consensus	Consensus + Behavioral Analytics
Data Privacy	High (but siloed)	Variable (ZKP required)	High (ZKP + AI encryption)
Fraud Risk	High (Forgery/Hacking)	Low (Immutability)	Near Zero (Proactive Detection)
Verification Speed	Days to Weeks	Seconds	Instantaneous
Primary Reference	Sharwani & Melo, (2024)	Berrios Moya *et al.* (2025)	Ghadi *et al.* (2025)

3. Methodology

Research Design

The methodology of this report employs qualitative analysis from a meta-analysis and case study perspective. Following Yin's, (2018) framework, case study research is especially useful during the investigation of contemporary phenomena that need to be placed in their real-world context and where the boundaries of the phenomenon and the context are not clearly visible.

Search Strategy and Sampling

The sampling method follows that of Xiao and Watson, (2019). Phase 1 focused on sampling high-impact journals and conferences spanning 2018-2026. "Blockchain academic verification," "transcript fraud USA," and "smart contracts education," were the employed terms. The sampling further focused on the PRISMA 2020 statement (Page *et al.*, 2022) for clarity and replicability in the selection procedures.

Data Collection and Quality Assessment

Following the findings of Brereton *et al.* (2007) concerning SLR in software engineering, this study divided data into three categories: technical, administrative, and legal. The Snyder (2019) tool was used to analyze whether research objectives were clearly stated and whether the research design and conclusion were sufficiently defended. This systematic approach helped the researcher stay focused on the technical issues in blockchain and maintain awareness of the other aspects related to the socio-technical issues.

Data Analysis

Data was analyzed using thematic synthesis. This involved coding the literature to find barriers and enablers. Annamalah *et al.* (2025) outline the need for case study research to maintain rigor and relevance. This was accomplished by triangulating technical publications (Patel & Das, 2019) with social and technical frameworks (Alammary *et al*., 2019) to provide a complete picture of the U.S. landscape.

Inclusion/Exclusion Criteria

Criterion	Inclusion Criteria	Exclusion Criteria
Geographical Focus	United Kingdom (England, Scotland, Wales, and Northern Ireland).	International studies (e.g., USA, Australia) unless providing comparative theory.
Setting / Context	Educational settings (Primary, Secondary, and Further Education).	Clinical health, youth justice, or purely social work settings with no school link.
Timeframe	Documents published between 2011 (Munro Review) and 2025.	Outdated statutory guidance superseded by newer versions (e.g., pre-2021 KCSIE).
Source Type	Peer-reviewed journals, statutory guidance, SCRs, and inspection reports.	Anecdotal blogs, news articles, or unverified non-academic opinion pieces.
Language	English language publications only.	Non-English language documents.

Table 2: Methodological Framework Comparison.

Methodology Phase	Applied Principles	Primary Methodological Reference
Review Strategy	Systematic Literature Review (SLR)	Xiao & Watson (2019)
Selection Rigor	PRISMA 2020 Standards	Page *et al.* (2022)
Case Study Design	Exploratory/Descriptive	Yin (2018)
Synthesis Method	Thematic Coding & Triangulation	Snyder, (2019); Annamalah *et al.* (2025)
Lessons Applied	Quality in Technical Documentation	Brereton *et al.* (2007)

Thematic Findings from the Literature Review

Theme 1: The Immutability Paradox and Security (Addressing RQ1)

The first main finding of RQ1 shows how the decentralization of blockchain removes the 'single point of failure'. According to Alammary *et al.* (2019), the distributed ledger shows that if one of the university servers fails, the global record will not get compromised. Nevertheless, there is a critical contradiction in the literature: while it is immutable and cannot be tampered with, this also means that legitimate administrative mistakes also cannot be corrected. Berrios Moya *et al.* (2025) suggest one of the solutions may be the use of 'revocation hashes' or 'update transactions' which allow a record to be updated to reflect the current truth while keeping the record history. Additionally, the use of multilevel blockchains which is proposed by Na and Park, (2022) can be viewed as a compromise providing a security and protection model for the data from its origin (in IoT sensors) to its storage, preserving the authenticity of the data from its origin.

Theme 2: Automation through Smart Contracts (Addressing RQ2)

Moving beyond RQ2, smart contracts offer administrative assurance as discussed in the literature. James, (2025) and (Patel and Das, 2019) explain that once a student finishes a course, smart contracts write to the ledger, and transcripts get updated. This almost completely eradicates transcript padding (or unauthorized grade modification) by administration. However, there seems to be a cost/benefit barrier as the complexity of writing such contracts presents a conundrum. As per Ghadi *et al.* (2025), the prediction is that such contracts will be written supplemented by AI, in code, and a preventive audit to ensure that such contracts do not have loopholes that can be exploited

by attackers. The combination of smart contracts and IoT (Na & Park, 2022; Mohammadiounotikandi and Babaeitarkami, 2024) may further automate the assurance of presence and/or participation, and therefore, a further level of prevention of fraud.

Theme 3: Legal, Technical, and Socio-Technical Barriers (Addressing RQ3)

The answer to RQ3 comprises several facets. From a legal standpoint, the main barrier is the absence of a national standard for digital identity in the USA. Walters and Takman, (2026) posit that, in the absence of a legal framework for cross-border data, US organizations run the risk of establishing 'digital islands' a collection of systems within an organization that cannot interoperate with each other within the USA. From a technical standpoint, the predominant barrier is still 'scalability and storage'. Delgado-von-Eitzen *et al.* (2021) argue that it is inefficient to store complete academic records on-chain, and the evidence supports a move to on-chain storage of hashes and off-chain storage of the complete records. The last barrier is the socio-technical readiness described by Sovtić *et al.* (2025), which suggests that the end of inertia and the high cost of initial migration are greater barriers compared to technology. This theme supports the notion that the greatest hurdles are legislative and cultural, rather than cryptographic.

4. Results and Discussion

Summary of Thematic Findings

This research has shown that blockchain technology provides a radical solution to transcript fraud in the USA. The automation of smart contracts reduces administrative fraud but comes at the cost of extremely high technical accuracy. The final analysis shows that the technology is advanced, but the US regulatory and legal frameworks have not yet matured to the extent that decentralized credentialing serves a purpose. Prior to this, the integration of AI and IoT provides a predictive and hardware-verified layer to the defense mechanism.

Research Reflections

The literature indicates a shift from "Can we use blockchain?" to "How can we use blockchain securely?" The addition of sources from 2025 and 2026 reflects an increasing concern for the intersection of blockchain with AI and IoT. The "smart" ecosystem of the future will mean that verification will happen continuously rather than in a single instance. The research method used, particularly the PRISMA-based SLR, contributed to the strength of the conclusions and supported findings through literature review, high-quality and peer-reviewed sources. The literature review shows that U.S. higher education system is at a tipping point, where the cost of disruption from stagnation will soon exceed the cost of disruption from technological change.

Advice to Regulators and US Law Schools

While the focus of the research is the USA, there are implications for other regulators around the globe and professional schools, including in the US. Regulators should consider a "Safe Harbor" for institutions using blockchain if certain encryption and ZKP requirements are met. Given the importance of institutional blockchain in securing the integrity of students' academic transcripts for bar admission, law schools should be the first to implement "Consortium Blockchains." This will create an industry standard that can be implemented in all areas of academia. Law schools in the UK must implement this standard to, at a minimum; enable the movement of lawyers between the UK and the USA.

5. Conclusion

Blockchain technology may hold the best possibility for achieving a fraud-free academic environment in the United States. By decoupling degree certification from centralized systems, and shifting to decentralized student ledgers, educational institutions can preserve the value of their degrees. Such a transformation relies on more than the capabilities of contemporary technology. Collaboration to establish a paradigmatic shift toward standards and legislation to balance privacy with transparency will be required. In the absence of significant national standards addressing privacy and transparency with respect to transcripts, innovations in higher education, particularly in the United States, may succeed in eliminating transcript fraud, while also granting students a lifelong, portable record of learning that is both safe and secure, as well as universally acceptable and beyond mathematical refutation. The continuous advancement of Blockchain

Technology, as well as AI and the IoT, lends support to the proverbial "single source of truth," and will offer the necessary immunity to more sophisticated threats and frauds in the Age of Digital Disruption.

6. Acknowledgment

I would like to thank the supervisors and instructors for technical insights, support and administrative data during the research stages of this systematic review, and the university.

7. Conflicts of Interest

I do not have a financial or personal conflict of interest that could prejudice the outcome or otherwise be interpreted as influencing or biasing the findings of this manuscript.

8. References

Alammary, A., Alhazmi, S., Almasri, M. and Gillani, S. (2019) 'Blockchain-based applications in education: A systematic review', *Applied Sciences*, **9**(12), p. 2400.

Al-Samarai, B. and 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), p. 2404.

Annamalah, S., Aravindan, K.L., Ahmed, S. and Sentosa, I. (2025) 'Exploring the relevance and rigour of case study research in business: a contemporary perspective', *Journal of Sustainability Research*, **7**(2).

Berrios Moya, J.A., Ayoade, J. and Uddin, M.A. (2025) 'A zero-knowledge proof-enabled blockchain-based academic record verification system', *Sensors*, **25**(11), p. 3450.

Brereton, P., Kitchenham, B.A., and Khalil, M. (2007) 'Lessons from applying the systematic literature review process within the software engineering domain', *Journal of Systems and Software*, **80**(4), pp. 571-583.

Camilleri, A.F. (2017) *Blockchain in education*. Joint Research Centre (JRC), the European Commission.

Chen, G., Xu, B., Lu, M. and Chen, N.S. (2018) 'Exploring blockchain technology and its potential applications for education', *Smart Learning Environments*, **5**(1), p. 1.

Delgado-von-Eitzen, C., Anido-Rifón, L. and Fernández-Iglesias, M.J. (2021) 'Application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information', *Applied Sciences*, **11**(10), p. 4537.

Fedorova, E.P. and Skobleva, E.I. (2020). 'Application of blockchain technology in higher education', *European Journal of Contemporary Education*, **9**(3), pp. 552-571.

Fleener, M.J. (2022). 'Blockchain Technologies: A Study of the Future of Education', *Journal of Higher Education Theory & Practice*, **22**(1).

Ghadi, Y.Y., Mazhar, T., and Hamam, H. (2025). 'A hybrid AI-Blockchain security framework for smart grids', *Scientific Reports*, **15**(1), p. 20882.

Gräther, W., Kolvenbach, S., and Wendland, F. (2018). 'Blockchain for education: lifelong learning passport', in *Proceedings of 1st ERCIM Blockchain workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).

James, M. (2025). Smart Contracts for Automated Academic Processes: Enrollment, Fees, and Transcript Management.

Marnita, M., Safarati, N., Bensaadi, I. and Taufiq, M. (2025). 'Blockchain-Based Credentialing for Teachers: A Systematic Literature Review on Transparency and Trust in Educational Management', in *Proceedings of The International Conference on Computer Science, Engineering, Social Science, and Multi-Disciplinary Studies*, 1, pp. 27-34.

Mohammadiounotikandi A., and Babaeitarkami S. (2024). The ethics of artificial intelligence: balancing progress with responsibility, *Int. J. Mat. Math. Sci*., **6**(2), 30-37. https://doi.org/10.34104/ijmms.024.030037

Na, D. and Park, S. (2022) 'IoT-chain and monitoring-chain using multilevel blockchain for IoT security', *Sensors*, 22(21), p. 8271.

Page, M.J., McKenzie, J.E., and Chou, R. (2022). 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *Revista Panamericana de Salud Publica*, **46**, p. e112.

Patel, K. and Das, M.L. (2019). 'Transcript management using blockchain enabled smart contracts', in *International Conference on Distributed Computing and Internet Technology*. Cham: Springer International Publishing, pp. 392-407.

Raimundo, R. and Rosário, A. (2021) 'Blockchain system in the higher education', *European Journal of Investigation in Health, Psychology and Education*, **11**(1), pp. 276-293.

Sharwani, A.E. and Melo, R. (2024) 'Blockchain-enabled academic credential verification in the USA', *Adhyayan: A Journal of Management Sciences*, **14**(02), pp. 31-41.

Snyder, H. (2019) 'Literature review as a research methodology: An overview and guidelines', *Journal of Business Research*, **104**, pp. 333-339.

Sokhandan A. (2024). Investigating the simultaneous performance of AI and Blockchain on E-banking transactions, *Int. J. Mat. Math. Sci*., **6**(2), 14-21. https://doi.org/10.34104/ijmms.024.014021

Sovtić, D., Trpkov, A., and Labus, A. (2025) 'Examining Readiness to Buy Fashion Products Authenticated with Blockchain', *Journal of Theoretical and Applied Electronic Commerce Research*, **20**(2), p. 119.

Sun, S., Du, R., Chen, S. and Li, W. (2021) 'Blockchain-based IoT access control system: towards security, lightweight, and cross-domain', *IEEE Access*, **9**, pp. 36868-36878.

Usama, M., Aziz, A., and Rehman, M.U. (2026). 'Blockchain-enabled identity management for IoT: a multi-layered defense against adversarial AI', *Scientific Reports*, **16**(1), p. 4371.

Walters, R. and Takman, L. (2026). 'Transnational personal data flows and blockchain technology', *Information & Communications Technology Law*, pp. 1-20.

Xiao, Y. and Watson, M. (2019). 'Guidance on conducting a systematic literature review', *Journal of Planning Education and Research*, **39**(1), pp. 93-112.

Yin, R.K. (2018). Case study research and applications. 6th edn. *Thousand Oaks, CA: Sage*.

Citation: Akter S. (2026). Blockchain technology for academic credential verification preventing transcript fraud in the USA. *Aust. J. Eng. Innov. Technol.*, **8**(4), 338-345.https://doi.org/10.34104/ajeit.026.03380345