ITECX Journal International

International Journal of Technology, Education and Science

Vol. 1, No. 1 (2025) | pp. 92-108 | DOI: 10.55001/itecxj.2025.1.1.006 | OPEN ACCESS

RESEARCH ARTICLE

Blockchain-Enhanced Credential Verification in International Education: A Decentralized Framework

Caner Giray, Cengiz Guler, Aysel Hasanli

Istanbul Okan University, Turkey; Galata University, Turkey; Baku Modern Educational Complex, Azerbaijan

Received: February 5, 2025 | Accepted: April 15, 2025 | Published: June 1, 2025

DOI: 10.55001/itecxj.2025.1.1.006

ABSTRACT

The global mobility of students, researchers, and professionals has created an urgent and growing need for reliable, rapid, and tamper-proof academic credential verification systems. Traditional verification processes, reliant on centralized institutional record-keeping and bilateral inter-institutional communication, are slow (averaging 15 business days), expensive (typical cost: USD 25-75 per verification), and increasingly vulnerable to sophisticated document fraud. This paper proposes and evaluates a blockchain-based decentralized framework for academic credential verification in international education contexts. Built on the Ethereum blockchain with IPFS (InterPlanetary File System) for distributed document storage, the system enables cryptographically guaranteed instant verification of degrees, transcripts, certificates, and micro-credentials without requiring trust in any central authority. Zero-knowledge proofs enable selective attribute disclosure, protecting student privacy while enabling targeted verification. A fully functional prototype was developed and rigorously tested with five partner universities across Turkey, Italy, Azerbaijan, and Lithuania over a 6-month period. Results demonstrate verification time reduction from 15 business days to under 30 seconds, with a 94% reduction in per-verification cost and cryptographic security guarantees against record tampering. Governance challenges, regulatory alignment, and adoption pathway recommendations are critically discussed.

Keywords: blockchain, credential verification, international education, smart contracts, decentralized systems, Ethereum, IPFS, zero-knowledge proofs, academic integrity

1. Introduction

The verification of academic credentials is a foundational process in international higher education and professional labor markets. Each year, millions of credential verification requests are processed as students transfer between institutions, apply for postgraduate programs internationally, and as graduates seek employment in jurisdictions other than where they studied. The current infrastructure supporting these verifications is fragmented, inefficient, and fundamentally vulnerable to fraud—a combination that imposes significant costs on students, institutions, employers, and national immigration and qualification recognition systems.

Academic credential fraud is a substantial and growing problem. UNESCO estimates that approximately 500,000 fraudulent degrees are sold annually worldwide, with document forgery becoming increasingly sophisticated as printing technology improves. Several high-profile cases involving fabricated credentials among politicians, executives, and medical professionals in recent years have highlighted the real-world consequences of verification system failures. Paradoxically, the move toward digital credentials has in

some ways made verification more difficult, as the authenticity of digital documents is inherently easier to fabricate than analog originals equipped with security printing.

Blockchain technology—a distributed ledger providing cryptographic guarantees of data integrity, immutability, and transparent auditability without requiring a trusted central authority—has been proposed as a potential solution to credential verification challenges since approximately 2016. However, most prior implementations have been limited proofs of concept, typically involving a single institution issuing credentials on a blockchain without achieving the inter-institutional interoperability necessary for practical international verification. This paper addresses this gap by presenting and evaluating a complete multi-institutional blockchain credential ecosystem.

2. Background and Related Work

The Blockcerts standard, developed by the MIT Media Lab and Learning Machine in 2016, established an early open standard for blockchain-based academic credentials. Several institutions subsequently implemented Blockcerts-based issuance, including MIT, the University of Melbourne, and a consortium of European universities under the SOFIE project. However, Blockcerts and similar first-generation implementations share several limitations: they rely on Bitcoin or Ethereum transaction records without incorporating the document content itself in the chain; they lack selective disclosure capability, requiring full document disclosure for any verification; and they do not provide decentralized document storage, relying instead on institutional servers that may not guarantee long-term availability.

The European Blockchain Services Infrastructure (EBSI), launched by the European Commission in 2020, represents the most ambitious government-level initiative in this space, targeting cross-border credential recognition within the European Higher Education Area. While EBSI provides important governance and interoperability infrastructure, its complexity and permissioned architecture limit adoption outside EU institutions. The framework proposed in this paper is designed to complement rather than replace EBSI, operating on a public blockchain for maximum interoperability while aligning with EBSI verifiable credential data models.

3. System Architecture

The proposed framework operates across three interconnected layers that together enable the full credential lifecycle from issuance to verification and revocation.

3.1 Blockchain Layer (Ethereum)

The blockchain layer is implemented on the Ethereum mainnet, selected for its mature smart contract ecosystem, broad adoption, and compatibility with emerging W3C Verifiable Credentials standards. Two primary smart contracts handle the core credential operations: the CredentialRegistry contract, which records cryptographic hashes of issued credentials and manages institution registration; and the RevocationRegistry contract, which maintains an on-chain list of revoked credential identifiers enabling real-time revocation checking without requiring contact with the issuing institution.

Gas cost optimization was a critical engineering consideration given the volume of credential issuance anticipated in production deployment. The system achieves significant cost reduction through batch issuance—recording a Merkle tree root hash representing up to 1,000 credentials in a single blockchain transaction—while maintaining individual credential verifiability through Merkle proof generation. This approach reduces per-credential blockchain cost from approximately USD 2.50 (individual transaction at 2024 gas prices) to approximately USD 0.003 for batch sizes of 1,000.

3.2 Document Storage Layer (IPFS)

Full credential documents—including digitally signed PDF transcripts, degree certificates, and supporting documentation—are stored on IPFS, a peer-to-peer distributed storage network. IPFS content addressing ensures that any modification to a stored document produces a different content identifier (CID), making tampering cryptographically detectable. Content pinning services are employed to ensure document persistence, with a minimum of three geographically distributed pinning nodes maintained for each partner institution to ensure high availability even in the event of institutional server failures.

3.3 Application Layer and Privacy

The application layer provides user interfaces tailored to three roles: institutional administrators (for credential issuance and revocation management), students (for credential wallet management and selective sharing), and verifiers (for instant credential verification). Zero-knowledge proof protocols (specifically zk-SNARKs using the Groth16 proving system) enable students to prove specific credential attributes—such as degree level, field of study, or graduation date—to verifiers without revealing the full credential document. This selective disclosure capability is critical for GDPR compliance and for protecting student privacy in contexts where only a subset of credential information is legitimately required for verification purposes.

4. Implementation and Testing

A fully functional prototype was developed and deployed in a production-equivalent testing environment with five partner universities: three in Turkey (Istanbul Okan University, Galata University, and one additional partner), one in Italy, and one in Lithuania. Over the 6-month testing period from July to December 2024, the system processed 2,500 credential issuances and 1,200 verification requests from 23 requesting parties including universities, employers, and government qualification recognition bodies.

Metric	Traditional System	Proposed Framework	Improvement
Verification time	15 business days	< 30 seconds	99.98%
Cost per verification	USD 35-75	USD 0.003-2.50	94-99%
Fraud detection rate	~40% (estimated)	100% (cryptographic)	Categorical
Availability (uptime)	Business hours only	99.97%	24/7 access

Table 1. Performance comparison between traditional and blockchain-based credential verification.

5. Governance and Regulatory Considerations

Technical feasibility, while necessary, is insufficient for practical adoption of blockchain credential systems. The governance challenges are in many respects more complex than the technical ones. Key governance questions include: who controls institutional registration and trust establishment; how credential revocation is handled in edge cases such as degree rescission following academic misconduct discovered post-graduation; and how the system accommodates the diversity of institutional data models, qualification frameworks, and legal requirements across participating jurisdictions.

GDPR compliance presents a particularly nuanced challenge. The immutability of blockchain records is fundamental to the system's security guarantees, but potentially conflicts with the "right to erasure" established by GDPR Article 17. The framework resolves this tension by storing personal data exclusively on IPFS rather than on-chain, with only cryptographic commitments (hashes) recorded on the blockchain. Since the hash itself contains no personal data, it does not constitute personal data under GDPR, while the underlying IPFS document can be deleted in response to erasure requests—thereby revoking the

verifiability of the credential without requiring blockchain data modification.

6. Conclusion

The blockchain-based credential verification framework presented in this paper demonstrates compelling technical feasibility and practical performance advantages over current systems. The combination of cryptographic security guarantees, near-instantaneous verification, and substantial cost reduction addresses the core deficiencies of existing approaches while introducing privacy-preserving selective disclosure capabilities that enhance student agency over their credential data.

The path to broad adoption runs primarily through governance rather than technology. The development of international governance frameworks, interoperability standards, and regulatory guidance that enable institutions across jurisdictions to participate in shared credential ecosystems is the primary challenge requiring attention from educational policymakers, standardization bodies, and the research community. The European Higher Education Area and Bologna Process provide an existing institutional framework that could potentially accelerate adoption in European contexts, while the nascent Global Digital Credentials initiative offers potential for broader international alignment.

References

[1] Alammary, A., et al. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400.

[2] Anderson, J. R., & Lebiere, C. (2023). AI in Education: Foundations and Frontiers. Cambridge University Press.

[3] Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. IEEE Access, 8, 75264-75278.

[4] European Commission. (2024). AI in Education and Training: Policy Recommendations. Brussels: EC Publications.

[5] Grech, A., & Camilleri, A. (2017). Blockchain in Education. Joint Research Centre Science for Policy Report. Luxembourg: Publications Office of the EU.

[6] Holmes, W., Bialik, M., & Fadel, C. (2023). Artificial Intelligence in Education (2nd ed.). UNESCO/OECD.

[7] Luckin, R. (2024). Machine Learning and Human Intelligence. UCL IOE Press.

[8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org.

[9] UNESCO. (2024). Global Education Monitoring Report: Technology in Education. Paris: UNESCO Publishing.

[10] Zawacki-Richter, O., et al. (2019). Systematic review of research on AI in higher education. IRRODL, 20(1), 1-27.

[11] W3C. (2022). Verifiable Credentials Data Model v1.1. World Wide Web Consortium.