American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Decentralized Credential Verification for Cross-Border Academic Mobility

Dr. Eleanor J. Peterson

Associate Professor, University of Copenhagen, Denmark

Abstract

Cross-border academic mobility depends heavily on the ability of universities, recognition authorities, employers, scholarship bodies, and public agencies to establish the authenticity and status of qualifications issued in other jurisdictions. Conventional verification frequently relies on paper documents, scanned certificates, institutional email correspondence, centralized databases, notarization, or specialized verification intermediaries. These processes can generate administrative delay, fragmented trust relationships, repeated disclosure of personal information, and difficulties when the original institution is slow to respond or its information systems have changed. The emergence of interoperable verifiable credentials provides an alternative architecture in which recognized institutions issue cryptographically secured academic claims to learners, who can store and present those credentials to receiving institutions while verifiers independently assess authenticity and credential status. The W3C Verifiable Credentials Data Model 2.0, published as a Recommendation in May 2025, formalizes an issuer–holder–verifier ecosystem for tamper-evident digital credentials, while 1EdTech Open Badges 3.0 and Comprehensive Learner Record 2.0 align educational achievement records with the W3C verifiable-credential model.

This paper develops a decentralized credential-verification framework for cross-border academic mobility. The proposed model integrates institutional trust registries, verifiable credentials, learner-controlled wallets, digital signatures, credential-status services, schema interoperability, recognition metadata, privacy protection, and conventional academic-recognition processes. A conceptual-methodological design is accompanied by a transparent simulation comparing conventional and decentralized verification across verification speed, portability, fraud resistance, learner control, interoperability, and administrative efficiency. The decentralized model receives higher illustrative scores across all six dimensions, although these values are methodological simulations rather than observed performance measures. The paper therefore argues for a layered architecture in which decentralized technology verifies evidence efficiently while qualified academic authorities retain responsibility for recognition decisions. Such a model can strengthen international mobility only when open technical standards are combined with trusted institutional governance, privacy-preserving presentation, revocation and status mechanisms, and fair recognition principles.

Keywords: verifiable credentials, academic mobility, decentralized identity, credential verification, higher education, digital diplomas, academic recognition, student mobility, blockchain, interoperability

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

International academic mobility increasingly requires institutions to exchange trustworthy evidence about education across national, institutional, linguistic, and technological boundaries. A student applying for postgraduate admission abroad may need to demonstrate a completed degree, course credits, grading information, accreditation status, identity, and sometimes individual learning outcomes. Traditionally, this evidence is transmitted through paper transcripts, sealed envelopes, certified copies, PDF files, institutional portals, email verification, or third-party credential-evaluation services. These approaches remain workable, but they can become slow and administratively expensive when receiving institutions need to contact foreign universities individually, determine whether documents are genuine, and reconcile qualification structures that differ across jurisdictions. European work on formal accreditation and recognition similarly describes conventional cross-university verification as time-consuming, costly, error-prone, and vulnerable to document fraud.

The development of verifiable digital credentials creates a different trust architecture. Under the W3C Verifiable Credentials Data Model 2.0, a credential contains claims made by an issuer and can be presented through an issuer–holder–verifier ecosystem in which cryptographic protection can make alteration detectable. The specification explicitly recognizes education certificates as a credential use case and addresses security, privacy, internationalization, and accessibility considerations. Educational interoperability standards have begun adopting the same architecture. 1EdTech states that Open Badges 3.0 credentials are digitally signed and compatible with the W3C Verifiable Credentials Data Model 2.0, while Comprehensive Learner Records can bundle multiple achievements into learner-controlled longitudinal records. This convergence is important because cross-border mobility depends not merely on digitization but on the ability of systems created by different institutions to interpret and verify one another's credentials.

Practical infrastructures are also emerging. European Digital Credentials for Learning provide verifiable digital versions of diplomas, training certificates, micro-credentials, and other learning achievements; credentials are electronically sealed and can be stored and shared through Europass-compatible wallets. Europass verification procedures are designed to allow viewers to assess origin, validity, and authenticity. The European Blockchain Services Infrastructure has similarly developed educational use cases in which universities issue diplomas and transcripts as verifiable credentials, students retain them in personal wallets, and receiving institutions can authenticate submitted credentials without repeatedly contacting the original issuer. The European Digital Identity Wallet framework also identifies academic credentials and university-related cross-border services among its intended use cases.

Nevertheless, technical verification and academic recognition are different activities. A cryptographically valid credential can establish that a particular issuer signed a particular claim and that the document has not been altered after issuance. It does not automatically establish that the issuer is a recognized higher-education institution, that the program possessed relevant accreditation, that the qualification is equivalent to a domestic award, or that the learning outcomes satisfy admission requirements. UNESCO's Global Convention on the Recognition of Qualifications concerning Higher Education emphasizes fair, transparent, and non-discriminatory recognition and provides an international framework within which qualifications are assessed for study and employment mobility. The

Convention entered into force in March 2022, and its operational guidelines adopted in 2025 provide practical support for institutions and credential evaluators. Decentralized credential verification should therefore strengthen recognition evidence rather than replace recognition expertise.

2. Objectives of the Study

2.1 To Develop an Interoperable Decentralized Verification Architecture

The first objective is to formulate an architecture through which universities can issue, learners can control, and receiving institutions can independently verify digital academic credentials across organizational and national boundaries. The framework incorporates W3C-compatible verifiable credentials, digital signatures, trusted issuer information, schema validation, credential-status mechanisms, learner wallets, and machine-readable educational metadata.

2.2 To Distinguish Credential Authenticity from Academic Recognition

The second objective is to establish a clear separation between technical authenticity and substantive qualification recognition. Cryptographic verification can answer whether a credential was issued by the claimed authorized entity and whether its integrity remains intact. Recognition processes must separately determine institutional legitimacy, qualification level, academic content, learning outcomes, credit equivalence, and compliance with admission or professional requirements.

2.3 To Evaluate Expected Advantages and Governance Risks

The third objective is to assess the potential performance of decentralized credential verification across six dimensions: verification speed, cross-border portability, fraud resistance, learner control, interoperability, and administrative efficiency. The study also examines governance risks involving issuer-key compromise, revocation, wallet loss, metadata inconsistency, surveillance, excessive disclosure, dependence on technical standards, and unequal institutional readiness.

3. Review of Literature

3.1 Verifiable Credentials and Decentralized Academic Identity

The contemporary verifiable-credential ecosystem represents a significant shift from document-centered verification toward cryptographically verifiable claims. W3C Verifiable Credentials Data Model 2.0 defines an extensible model in which an issuer makes claims, a holder manages credentials, and a verifier evaluates presentations. The standard is intended to make credentials tamper-evident while preserving extensibility across domains, including education. Verifiable Credential Data Integrity 1.0 complements the data model by specifying cryptographic mechanisms for securing authenticity and integrity through digital signatures and related proofs.

Credential lifecycle management is equally important. A genuine credential can later become invalid because it was issued in error, superseded, suspended, or revoked. The W3C Bitstring Status List 1.0 Recommendation provides a privacy-oriented and space-efficient mechanism through which credential status such as suspension or revocation can be published and checked. This capability is particularly relevant to academic mobility because a credential must remain verifiable years after issuance without forcing receiving institutions to depend on manual email confirmation.

Decentralized identifiers can provide an additional trust mechanism where appropriate. W3C's DID work describes decentralized identifiers as identifiers designed to support cryptographically verifiable digital identity while allowing implementations to reduce dependence on centralized identity providers or registries. A university, accreditation body, learner, or other authorized entity can potentially be associated with an identifier whose cryptographic material is discoverable through the relevant method. However, decentralized credentials do not require every ecosystem to use the same DID method, and excessive methodological diversity can itself become an interoperability problem.

Higher-education research has explored numerous distributed credential systems. Saleh, Ghazali, and Idris proposed a decentralized certification-verification protocol designed to preserve privacy while supporting educational certificate issuance and verification. Le and colleagues subsequently proposed IU-TransCert, a blockchain-based academic credential architecture designed around issuance, verification, auditing, and an auditable Merkle-tree structure. More recent systems such as BlockAdemiC continue investigating distributed educational credential management and verification. Collectively, this literature demonstrates considerable technical interest, but practical international mobility requires standards and institutional trust mechanisms that extend beyond an individual blockchain implementation.

3.2 Educational Standards, Wallets, and Cross-Border Portability

Education-specific standards are important because generic credentials do not automatically contain the semantic information needed for admission and recognition. Open Badges 3.0 provides structured metadata describing achievements, issuers, earners, criteria, and supporting evidence and is compatible with the W3C Verifiable Credentials model. Comprehensive Learner Record 2.0 allows multiple achievements to be represented as longitudinal learner records. These standards are relevant to mobility because learners increasingly carry not only complete degrees but also micro-credentials, professional learning, short courses, and competency evidence.

European Digital Credentials for Learning illustrate how a large-scale public infrastructure can combine educational semantics with trusted digital signatures. Europass describes EDCs as verifiable digital learning credentials that can include diplomas, certificates, micro-credentials, and other achievements. They can be held in compliant wallets and shared directly for employment, further learning, and recognition procedures. In June 2020, Europass further emphasized that holders can store, verify, and share such credentials across borders through supported tools.

EBSI's education architecture illustrates a more decentralized verification workflow. Its current infrastructure is based on open standards and is designed so that institutions, employers, and public bodies can verify credentials issued elsewhere without requiring repeated bilateral integration between every pair of organizations. The Formal Accreditation and Recognition project demonstrates a scenario in which a learner requests a bachelor's degree and transcript as verifiable credentials, stores them in a personal wallet, consents to presentation when applying abroad, and enables the receiving university to verify authenticity automatically before continuing with substantive academic evaluation.

3.3 Recognition Governance, Privacy, and Remaining Research Gaps

Authenticity solves only part of the mobility problem. International recognition operates through national authorities, accreditation structures, institutional policies, qualification frameworks, and conventions. UNESCO's Global Convention establishes principles for fair, transparent, and non-discriminatory recognition and explicitly supports mobility across borders, including recognition of non-traditional forms of learning. A decentralized credential ecosystem should therefore expose enough structured information to support recognition while avoiding the false assumption that machine verification can resolve complex academic equivalence automatically.

Privacy represents a second major concern. Academic credentials often contain more information than a verifier requires. A receiving university may need confirmation that a person holds a bachelor's degree in a specified field but may not need a complete transcript at the initial application stage. Modern verifiable-credential approaches increasingly support selective disclosure. W3C's JOSE and COSE specification includes mechanisms for selective-disclosure representations, while BBS cryptosuites are designed to enable derived proofs that reveal only selected claims. These capabilities can reduce unnecessary exposure when implemented correctly.

Issuer trust remains a difficult governance problem. A cryptographic signature proves that a credential corresponds to a particular cryptographic key; the verifier must still establish whether that key represents a legitimate recognized university. Trust registries, accreditation records, qualified electronic seals, issuer metadata, and recognized authorities therefore remain necessary. EBSI's current model attempts to address this by connecting verifiable credentials to a European trust infrastructure rather than leaving every verifier to decide independently which keys are authoritative.

4. Research Methodology

4.1 Research Design and Evidence Base

The study adopts a conceptual-methodological design with simulation-based comparative analysis. No real student applications, university admission records, credential-verification logs, or personal educational records were collected. Numerical values reported in Section 5 were created solely to demonstrate the comparative framework.

The methodological synthesis draws principally from current open technical specifications and public credential infrastructures. W3C Verifiable Credentials Data Model 2.0 provides the generic issuer–holder–verifier architecture; Verifiable Credential Data Integrity and Bitstring Status List support integrity and lifecycle management; 1EdTech standards provide education-specific achievement structures; Europass and EBSI provide operational institutional examples; and UNESCO's Global Convention provides the normative recognition framework.

The methodology therefore evaluates decentralized credentials as recognition-support infrastructure, not as an autonomous qualification-recognition system.

4.2 Proposed Cross-Border Credential Verification Architecture

The proposed workflow contains seven connected components: recognized issuer, credential issuance service, learner-controlled wallet, interoperable credential schema, trust registry, status service, and verifier/recognition authority.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 1: Governance Architecture for Decentralized Cross-Border Academic Credential Verification

Architectural Component	Core Function	Required Governance Control	Principal Mobility Benefit
Recognized Academic Issuer	Creates authoritative qualification claims	Institutional accreditation and issuer authorization must be independently discoverable	Establishes trusted origin
Verifiable Credential	Encodes diploma, transcript, credits or micro-credential in machine-readable form	Common schema, cryptographic integrity and persistent identifiers	Reduces document tampering and manual re-entry
Learner Wallet	Stores and presents credentials under learner control	Secure recovery, consent, accessibility and portability	Enables learner-mediated mobility
Institutional Trust Registry	Establishes which issuers and accreditation authorities are recognized	Transparent governance, update process and jurisdictional authority	Separates valid issuers from fraudulent credential creators
Credential-Status Service	Publishes suspension, revocation or supersession information	Privacy-preserving status checking and high availability	Supports long-term validity checks
Receiving Institution / Verifier	Checks credential authenticity and relevant status	Standards-conformant verification and minimal data collection	Accelerates administrative verification
Academic Recognition Authority	Determines substantive equivalence and admission relevance	Transparent recognition criteria and qualified human/authorized institutional review	Preserves fairness and academic judgment

Source: Author-developed framework based on W3C verifiable-credential standards, 1EdTech educational credential specifications, Europass, EBSI, and UNESCO recognition principles.

The verification process can be represented conceptually as:

[Issuer \rightarrow Credential \rightarrow Holder \rightarrow Presentation \rightarrow Verifier \rightarrow Recognition]

Technical verification is expressed as:

[V_T = I_s \times S_g \times C_i \times C_s]

where (I_s) represents trusted issuer status, (S_g) represents valid cryptographic signature or proof, (C_i) represents credential integrity, and (C_s) represents acceptable credential status.

Academic recognition remains a distinct function:

[R_A = f(Q_l, A_s, L_o, C_r, J_p)]

where (Q_l) is qualification level, (A_s) is accreditation status, (L_o) is learning-outcome relevance, (C_r) is credit or curriculum relevance, and (J_p) represents the applicable jurisdictional or institutional recognition policy.

4.3 Comparative Simulation and Analytical Criteria

Two verification models were constructed. The Conventional Verification Model represents workflows dependent on scanned or paper documents, institutional correspondence, third-party checks, and manual record comparison. The Decentralized Credential Model represents standards-based digital credentials held by learners and verified through cryptographic proofs, trusted issuer information, machine-readable metadata, and status services.

Six normalized dimensions were assessed on a 0–100 scale. Verification speed concerns the time and administrative steps required to establish authenticity. Cross-border portability considers the ability to present the same credential across institutions and jurisdictions. Fraud resistance considers tamper detection and issuer authentication. Interoperability considers technical and semantic compatibility. Administrative efficiency considers repetitive verification workload and dependence on issuer-to-verifier correspondence.

5. Analysis

5.1 Comparative Verification Performance

Table 2: Simulated Comparison of Conventional and Decentralized Academic Credential Verification

Verification Dimension	Conventional Verification	Decentralized Credential Model	Simulated Improvement	Principal Explanation
Verification Speed	48	91	+43	Cryptographic verification can reduce repeated manual issuer contact
Cross-Border Portability	44	88	+44	Standards-based credentials can be presented to multiple compatible institutions
Fraud Resistance	63	92	+29	Digital signatures and issuer verification make

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

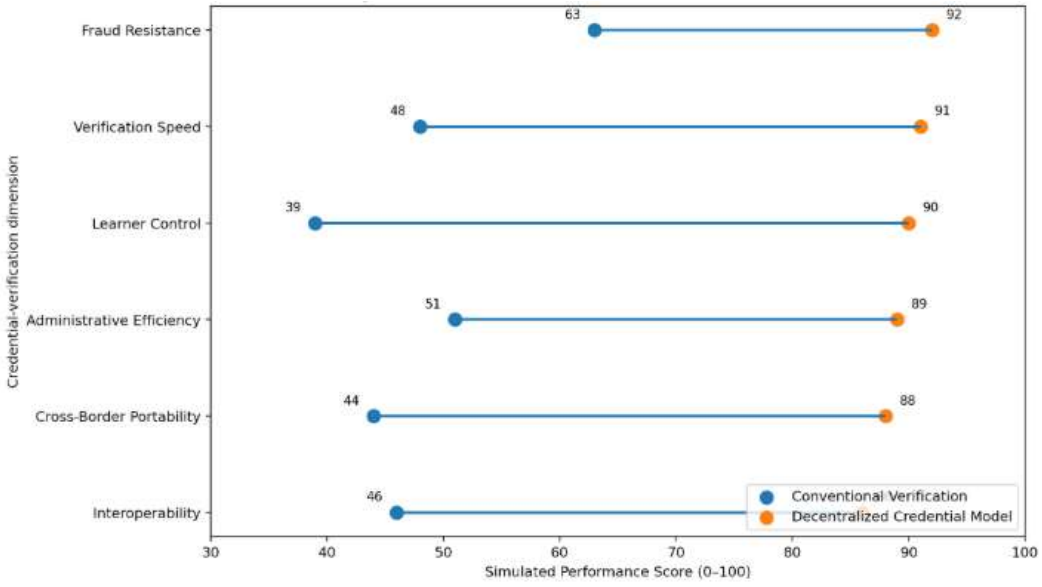
Verification Dimension	Conventional Verification	Decentralized Credential Model	Simulated Improvement	Principal Explanation
				unauthorized alteration detectable
Learner Control	39	90	+51	Holder-managed wallets enable direct presentation and consent
Interoperability	46	86	+40	Shared technical and educational schemas reduce institution-specific formats

Note: All scores are author-generated simulations and are not measurements from an operational university network.

The largest simulated improvement occurs in learner control. Conventional academic-verification processes often require institutions or external intermediaries to transmit records directly. In a holder-mediated model, the learner receives a credential and can present it repeatedly without altering the original issuer-signed information. European Digital Credentials for Learning already use a wallet-oriented model in which holders can store and share credentials for recognition and further learning..

5.2 Dumbbell Analysis of Verification Transformation

Graph 1: Simulated Comparison of Conventional and Decentralized Academic Credential Verification for Cross-Border Mobility



Source: Author-generated simulation.

The dumbbell graph highlights the gap between the two simulated verification approaches. The largest difference occurs in learner control, where the decentralized model shifts verification from institution-to-institution document exchange toward holder-mediated credential presentation. Portability and verification speed also demonstrate large differences because a digitally signed credential can theoretically be verified repeatedly without generating a new institutional verification request every time it crosses a border.

5.3 Proposed Decentralized Mobility Workflow

A learner completes a recognized academic program and the university creates a machine-readable credential containing the qualification name, institution, learner identifier or privacy-preserving subject reference, award date, relevant level information, and other necessary academic metadata. The institution signs or otherwise secures the credential using a standards-compliant cryptographic method. W3C's VC ecosystem explicitly supports digitally verifiable education credentials, while Open Badges 3.0 can represent degrees, skills, competencies, and micro-credentials through signed verifiable achievements.

The learner receives the credential into a compatible wallet. When applying to a foreign university, the applicant authorizes presentation of the relevant credential. Where the technology supports selective disclosure, only claims necessary for the transaction should be revealed rather than automatically disclosing the complete academic record.

6. Discussion

6.1 Decentralization Should Reduce Verification Dependence Without Eliminating Institutional Trust

The analysis suggests that the strongest argument for decentralized credential verification is not that trust can be removed from academic mobility. Higher education is fundamentally institutional: qualifications acquire meaning because recognized organizations award them under established academic and regulatory structures. Decentralization can instead reduce the number of occasions on which a receiving university must re-establish trust through direct bilateral communication with the issuer. Once an issuer is recognized through an appropriate trust framework and its credential is cryptographically verifiable, the receiving institution can validate the evidence independently and focus administrative resources on academic recognition. EBSI's current education model reflects this principle by enabling institutions to verify degrees and professional qualifications through a shared trust infrastructure without requiring a separate bilateral verification arrangement with every issuer.

This distinction is important because some blockchain-oriented credential proposals imply that immutability itself creates trust. It does not. A fraudulent institution can immutably record a fraudulent degree. A legitimate institution can mistakenly issue an inaccurate credential. A cryptographic system can prove that data were signed by a particular key without proving that the key belongs to an accredited university unless a governance mechanism establishes that relationship. Trusted issuer registries, accreditation records, qualified electronic signatures or seals, and recognized institutional identifiers are therefore essential parts of a decentralized academic ecosystem.

The architecture should also avoid unnecessary dependence on a single distributed ledger. W3C verifiable credentials are an interoperable credential data model rather than a mandate to store educational records on one particular blockchain. This flexibility is beneficial for cross-border mobility because national infrastructures, universities, and credential providers can use different underlying technologies while maintaining compatible credential formats and verification protocols. Decentralization is strongest when it provides interoperability and portability rather than replacing one centralized dependency with another global proprietary platform.

6.2 Learner Control Must Be Balanced with Privacy, Recovery, and Accessibility

Holder-controlled credentials can transform the student's position within academic mobility. Instead of repeatedly asking former institutions to send documents, learners can retain verifiable evidence and present it when required. Europass and EBSI educational credential models already illustrate this holder-mediated architecture. Such control can reduce administrative dependency and may be particularly beneficial for internationally mobile graduates who need to verify qualifications several years after leaving the issuing institution.

However, learner control should not be interpreted as requiring learners to become their own security administrators. Wallet loss, device theft, cryptographic-key loss, accessibility limitations, and technological exclusion can create new barriers. Universities and credential ecosystems therefore require well-designed recovery procedures. Recovery should not permit unauthorized parties to take control of credentials, but it should also not make an academic qualification permanently inaccessible because a graduate lost a mobile phone years after graduation.

Privacy requires equal attention. Digital portability can increase surveillance if every credential presentation reveals a stable global identifier or causes the issuer to learn every time a graduate presents a degree. Verification architectures should therefore minimize unnecessary correlation and limit disclosure to claims relevant to the receiving institution. W3C's contemporary credential ecosystem includes selective-disclosure approaches specifically intended to reduce unnecessary information exposure.

6.3 Technical Verification Can Accelerate Recognition but Cannot Automate Academic Judgment

The distinction between verification and recognition is the most important governance principle in the proposed framework. Technical verification answers whether the credential is authentic and currently acceptable according to its lifecycle status. Recognition answers whether the qualification should be accepted for a particular educational, professional, or legal purpose. UNESCO's Global Convention explicitly treats recognition as a fair and transparent institutional process rather than a purely documentary authentication task.

Consider a digitally verified bachelor's degree issued by a legitimate foreign university. A receiving university may still need to determine whether the degree provides adequate preparation for a master's program, whether prerequisite courses were completed, how the qualification maps to the domestic framework, and whether specific professional accreditation requirements apply. No digital signature resolves these questions.

The value of decentralized verification is therefore that it can remove lower-level uncertainty before academic evaluation begins. Recognition officers should spend less time deciding whether a transcript is forged and more time evaluating what the verified learning actually represents. The EBSI Formal Accreditation and Recognition model reflects this sequencing: credentials can be verified automatically before the foreign applicant proceeds into the academic evaluation stage.

7. Conclusion

Cross-border academic mobility depends on a reliable connection between educational achievement and institutional trust. Conventional credential-verification processes often establish that connection through repeated document exchange, manual institutional confirmation, certified copies, and third-party verification. These approaches remain important, but they can create delays and administrative costs when learners move across multiple institutions and jurisdictions. Verifiable credential technologies provide an alternative in which recognized institutions issue cryptographically protected academic records that can be held and presented by learners and independently verified by receiving organizations. The maturation of W3C Verifiable Credentials 2.0, education-specific standards such as Open Badges 3.0 and CLR 2.0, European Digital Credentials for Learning, and EBSI demonstrates that the technical foundations of such an ecosystem are becoming increasingly practical.

The study's simulated comparison suggests substantial potential improvements in verification speed, portability, learner control, interoperability, fraud resistance, and administrative efficiency. The strongest illustrative gain occurs in learner control because holder-mediated credentials reduce dependence on repeated institution-to-institution document transmission. Cross-border portability and verification speed also improve substantially when a receiving institution can authenticate a credential directly through standards-based cryptographic mechanisms. These values are methodological simulations rather than empirical measurements, but they demonstrate why decentralized credentials deserve serious consideration as mobility infrastructure.

The analysis also establishes clear limits. Cryptographic authenticity is not academic recognition, blockchain immutability is not institutional legitimacy, and learner control is not equivalent to privacy unless credential presentations are designed carefully. A responsible cross-border architecture requires recognized issuer governance, status and revocation mechanisms, interoperable educational metadata, secure wallet recovery, selective disclosure, accessibility, and transparent recognition procedures. International recognition frameworks remain essential because qualification equivalence depends upon academic and legal context, not simply document authenticity. UNESCO's Global Convention provides an important normative foundation for fair and transparent recognition across borders.

The most sustainable model is therefore a layered trust architecture. The issuer certifies achievement, open credential standards preserve machine readability, cryptographic mechanisms protect integrity, trusted registries establish legitimate institutional authority, the learner controls presentation, the verifier checks authenticity and status, and qualified recognition authorities determine academic meaning. Future empirical research should test this architecture through multinational university pilots, measure end-to-end verification time and administrative cost, evaluate selective-disclosure usability, examine wallet recovery and accessibility, and compare interoperability across W3C, 1EdTech, Europass, EBSI, and emerging national infrastructures. The objective should not be to eliminate

institutions from academic verification but to allow institutions to trust authentic evidence more efficiently while giving internationally mobile learners a secure, portable, and durable means of carrying their academic achievements across borders.

References

1. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org.
2. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
3. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.
4. Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.
5. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27
6. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
7. Allen, C. (2016). *The Path to Self-Sovereign Identity*. Life With Alacrity.
8. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access, 7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2939271
9. Preukschat, A., & Reed, D. (Eds.). (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning Publications.
10. Naik, N., & Jenkins, P. (2020). Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 90–95.
11. Fedorova, E. P., & Skobleva, E. I. (2020). Application of blockchain technology in higher education: A systematic review. *Education and Information Technologies, 25*, 303–312.
12. Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education*. Joint Research Centre, European Commission.
13. Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access, 6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929
14. Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. *Proceedings of the 11th European Conference on Technology Enhanced Learning*, 490–496. https://doi.org/10.1007/978-3-319-45153-4_48
15. Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments, 5*, 1. https://doi.org/10.1186/s40561-017-0050-x

16. Mikroyannidis, A., Okada, A., & Domingue, J. (2019). Blockchain for open recognition and certification in education. *Proceedings of the European Distance and E-Learning Network Annual Conference*, 1–10.
17. European Commission. (2019). *European Blockchain Services Infrastructure: Self-Sovereign Identity and Verifiable Credentials*. European Commission.
18. International Organization for Standardization. (2019). *ISO/IEC 18013-5: Personal Identification—ISO-Compliant Driving Licence—Part 5: Mobile Driving Licence Application*. ISO.
19. World Wide Web Consortium. (2021). *Verifiable Credentials Data Model 1.0*. W3C Recommendation.
20. World Wide Web Consortium. (2021). *Decentralized Identifiers (DIDs) v1.0*. W3C Working Draft.