RESEARCH ARTICLE WWW:IoJet.org

Blockchain-Based Credentialing in Online Education: Enhancing Trust, Verification, and Academic Transparency

Prasad Ghodke[1]*, Atul Vasudev Dusane[2], Tanveer Ahmad Wani[3], Bipin Sule[4], Yogesh B. Mandake[5], Rajendra Vasantrao Patil[6], Mahendran A[7]

[1]Assistant Professor, Department of MBA,Institute: Modern Institute of Business Studies Nigdi SavitribaiPhule Pune University Pune

[2]Assistant professor, Department of AIML, SVKM's NMIMS SHIRPUR Campus

[3]Professor, School of Sciences,Noida International University,Uttar Pradesh, India

[4]Department of Eengineering, Science and Humanities, Vishwakarma Institute of Technology, Pune, Maharashtra, India

[5]Assistant Professor, Department of Electrical and Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India

[6]Assistant Professor, Department of Computer Engineering, SSVPS Bapusaheb Shivajirao Deore College of Engineering, Dhule (M.S.)

[7]Center for Global Health Research,Saveetha Medical College, Saveetha Institute of Medical and Technical Sciences, Chennai, India

Keywords:

Blockchain Credentialing, Online Education, Credential Lifecycle, Verification Design, Conceptual Framework, Registrar Workflows

Author's Email :
prasadsppu1@gmail.com,
atul.dusane@nmims.edu,
tanveer.ahmad@niu.edu.in,
bipin.sule@vit.edu,
yogesh.mandake@bvucoep.edu.in,
patilrajendra.v@gmail.com,
mahendrana.sdc@saveetha.com

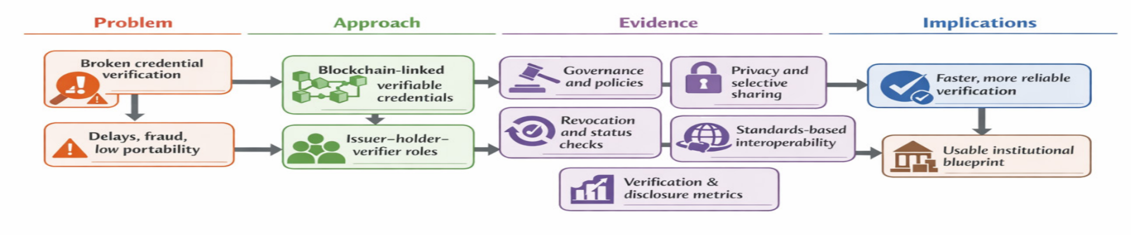
Abstract

Online education increasingly relies on digital credentials, yet fragmented record systems can lead to verification delays, increase fraud risk, and limit portability across institutions. Although blockchain is often presented in current discussions as the primary remedy, this emphasis can leave unresolved how roles, standards, governance, privacy, and revocation jointly determine trust and academic transparency. Against this background, this paper proposes a practical conceptual framework for blockchain linked credential workflows. It clarifies issuer, holder, and verifier responsibilities across the credential lifecycle and specifies what constitutes verification completeness, including issuer legitimacy, credential integrity, and revocation status. To differentiate transparency from unnecessary exposure, the framework also introduces disclosure minimization, which elaborates privacy preserving verification and bounds what transparency should mean in this setting. Overall, the contribution is a standards aware design and evaluation model that avoids cryptocurrency framing and low level cryptographic detail, while situating adoption constraints as central to implementation choices. The model is intended for educational technology researchers and inst itutional registrars who are designing online credential verification workflows.

Author's Orcid :
0009-0007-2194-1116,
0000-0002-7419-240X

Received : 08.03.2025
Revised : 16.06.2025
Accepted : 23.06.2025

How to cite this article: Ghodke P, Dusane AV, Wani TA, Sule B, Mandake YB, Patil RV, Mahendran A, Blockchain-Based Credentialing in Online Education: Enhancing Trust, Verification, and Academic Transparency. International Online Journal of Education and Teaching, Vol. 12, No. 3, 2025, 157-167


Problem
Approach
Evidence
Implications
Broken credential verification
Delays, fraud, low portability
Blockchain-linked verifiable credentials
Issuer–holder–verifier roles
Governance and policies
Privacy and selective sharing
Revocation and status checks
Standards-based interoperability
Verification & disclosure metrics
Faster, more reliable verification
Usable institutional blueprint

Graphical abstract

Introduction

Online education increasingly depends on digital credentials to represent learning that spans platforms, providers, and jurisdictions. However, verification is often slow and fragmented, and it remains vulnerable to misrepresentation. Learners and external verifiers such as employers therefore need assurance that a presented credential comes from a legitimate issuer, has not been altered, and remains valid at the time of use. Recent reporting on digital credential activity suggests that demand for reliable verification is increasing, so credential trust is becoming an operational concern rather than a distant possibility.[1] In this setting, each credential presentation should be checked at the point of use rather than accepted on presentation alone.[2] The near-term pressures shaping these risks and constraints are summarized in Fig. (1).

Because credentials are used outside the issuing institution, identity and verification operate as shared infrastructure that must function across systems and organizations, rather than as a local database feature.[2, 3] This study clarifies a disciplined conceptual

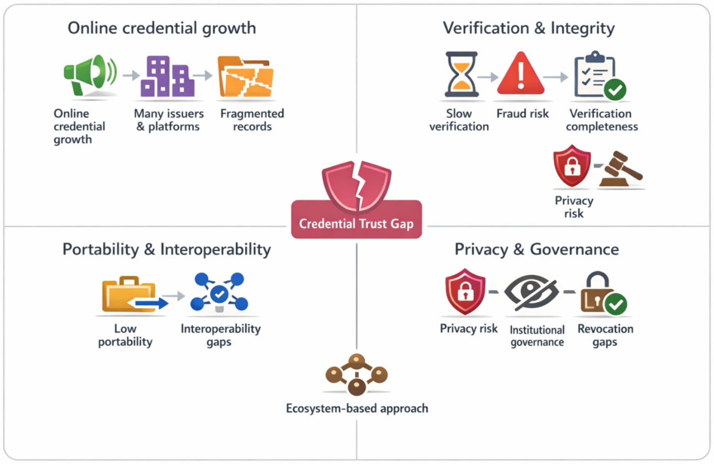


Fig. 1: Why-now credential trust landscape

framework for blockchain-linked credentialing in online education by situating issuer, holder, and verifier roles within the full credential lifecycle, from issuance through sharing and verification, and by differentiating the design requirements intended to keep records trustworthy while respecting privacy, interoperability, and revocation. In this paper, transparency is defined as auditable provenance and clear status, not unrestricted exposure of personal data. The framework is deliberately scoped to credential trust workflows and institutional governance boundaries, and it does not argue for cryptocurrency, speculative disruption narratives, or low-level cryptographic protocol design.

Credentialing problem world and domain framing

Online education credentialing operates in a setting where learning evidence, award decisions, and long-term records are spread across multiple systems and organizations. This fragmentation undermines routine verification because a verifier must rebuild the surrounding context, establish issuer legitimacy, and interpret heterogeneous formats before reaching a decision. Verification becomes more efficient when credential formats are standardized, issuing authorities are recognized, and checks are applied consistently across institutions.[4] Credentialing often lacks these shared structures, so verification becomes a case-by-case activity that does not scale well.

In practice, learners and credential consumers frequently encounter delays when transcripts, certificates, or micro-credentials require manual confirmation through registrars, platform providers, or third party services. These handoffs also define common failure modes for trust: when integrity signals are weak or inconsistently checked, a credential can be hard to validate or may be accepted after incomplete verification. Portability fails in similar ways when a credential cannot move cleanly from an issuing environment into another institutional or employer system without re-entry or ad hoc translation. Fig. (2) summarizes these high-friction handoffs and where verification work accumulates. Adoption therefore depends not only on technical integration but also on incentives for stakeholders to issue, hold, and verify credentials using shared rules and interfaces.[5]

Security, privacy, and audit requirements further intensify these challenges for regulated records, where institutions must manage exceptions, corrections, and access control while maintaining accountability.[4, 6] Tab. (1) maps four recurring pain points to the framework responses proposed in this study. Verification delays are framed as a workflow design issue and are addressed through a trusted, verifiable credential process organized around issuer-holder-verifier roles. Fraud risk is framed as a verification completeness failure that requires checking issuer legitimacy and credential integrity within auditable

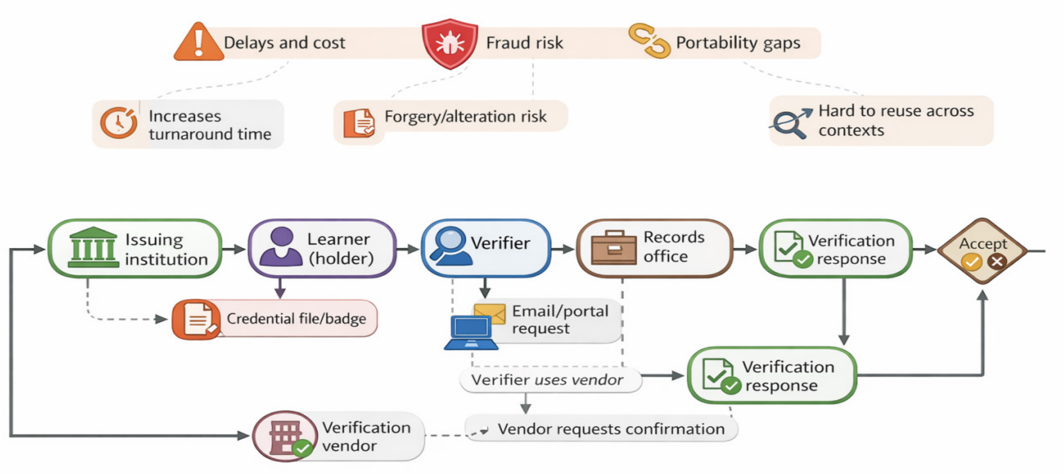


Fig. 2: Current credential verification process

Table 1: Pain points mapped to framework responses

Pain Point	What Goes Wrong	Framework Response
Verification Delays	Slow checks across fragmented record systems	Trusted, verifiable credential workflow with issuer-holder-verifier roles
Fraud Risk	Hard to confirm credential integrity and issuer legitimacy	Verification built around trust and verification logic, plus auditable processes
Portability Problems	Credentials do not move cleanly across institutions and systems	Interoperability focus and standards alignment for cross-system compatibility
Institutional Complexity	Technology alone cannot reflect institutional rules and adoption constraints	Governance and implementation logic tied to institutional rules, privacy, and revocation

processes rather than relying on presentation alone. Portability constraints motivate interoperability and standards alignment so credentials can be used across systems without rework. Institutional complexity motivates governance and implementation logic that links technical decisions to institutional rules, privacy requirements, and revocation handling.

Key Concepts, Actors, and Standards

Digital credentials are used as portable records of learning that can move across online education systems. Key terms, including verifiable credentials and revocation, are specified in Tab. (2). The workflow differentiates issuer, holder, and verifier roles and trust links in Fig. (3). Verification relies on evidence rather than presentation alone,[7] whereas additional identity-proofing requirements can introduce privacy risk and operational burden.[7, 8]

Roles and credential artifacts

Online credential workflows typically involve an issuer that signs a credential, a holder that controls storage and sharing, and a verifier that checks authenticity and status. The exchanged artifacts include the signed credential, a holder-generated presentation, and the identifiers and proofs that bind issuer and holder identities. Framing these interactions as a trust and verification workflow, rather than simple document exchange, clarifies the security and institutional requirements.[9] In line with this framing, verifiers can validate proofs locally when the credential design supports independent checking, which reduces reliance on central lookup services.[9, 10]

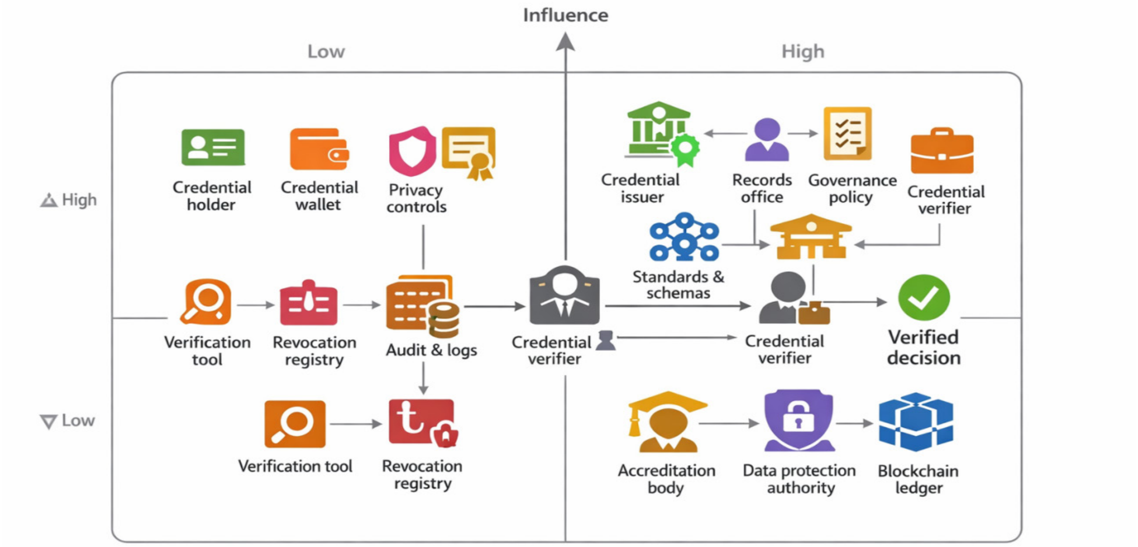


Fig. 3: Issuer-holder-verifier stakeholder roles

Table 2: Key credential terms and definitions

Term	Working Definition	Why It Matters
Digital Credentials	Digital records of learning used in online education	Core object being issued, shared, and verified
Issuer-Holder-Verifier	The main roles in the credential ecosystem: issuer creates credentials, holder presents them, verifier checks them	Organizes the workflow and clarifies who does what
Verifiable Credentials	A credential form designed to support verification	Supports trusted verification across systems and institutions
Revocation	Ability to revoke a credential and check its revocation status during verification	Needed for credible verification over time and for handling changes or corrections

Portability across institutions requires that a verifier can extend trust beyond a single organization, for example by chaining from the credential to an issuer authority that is recognized in another domain.[11] Practical portability therefore depends on stable issuer identifiers and keys, shared schemas that preserve meaning across platforms, and a revocation signal that remains checkable over time. Taken together, this view situates the credential object within cross-organization governance that defines who is trusted and under what conditions.

Verification, revocation, privacy, and standards touchpoints

Complete verification in online education must establish more than simple credential possession. The three checks summarized in Tab. (3) are issuer legitimacy, credential integrity, and revocation status. Issuer legitimacy clarifies whether the credential is traceable to the claimed institution or an authorized platform. Integrity requires that the credential contents match what was issued and have not been altered during storage or sharing. Revocation status verifies that a credential that was withdrawn or corrected is not mistakenly accepted as valid.

Revocation and privacy therefore function as core design requirements rather than optional features. A realistic workflow needs a revocation mechanism that propagates across systems, otherwise verification can fail by accepting outdated credentials, while still avoiding exposure of unnecessary personal data. Privacy, however, also constrains transparency, so verification should disclose only the minimum information needed for a decision. Standards alignment, including verifiable credential formats and institutional governance rules, bounds what can interoperate at scale.

Proposed Credential Ecosystem Framework

This study presents a design framework that situates digital credential trust in online education as an ecosystem of roles and lifecycle controls, rather than as a single blockchain feature.[12] It differentiates responsibilities across issuance, holding, sharing, verification, update, and revocation, linking these stages to actor accountability, disciplined key custody, and audit-friendly records across issuers, holders, and verifiers.[12, 13] The framework also

Table 3: Verification completeness required checks

Check Area	What To Confirm	Why It Matters
Issuer Legitimacy	Credential comes from the claimed issuer	Prevents acceptance of credentials from illegitimate sources
Credential Integrity	Credential content has not been altered	Protects the record against tampering after issuance
Revocation Status	Credential has not been revoked	Avoids accepting credentials that are no longer valid

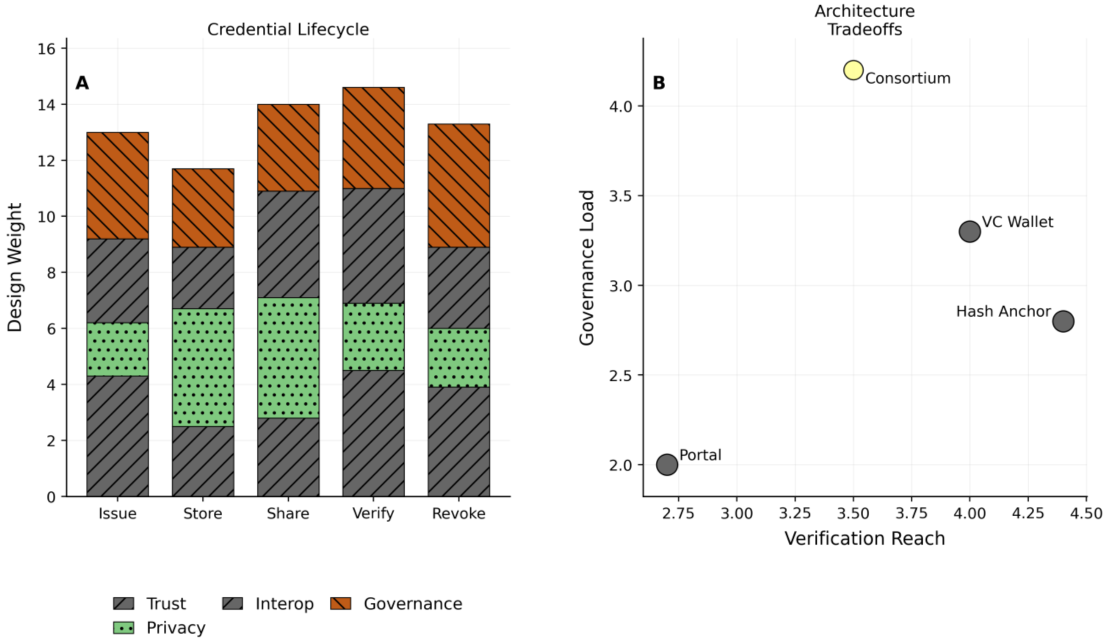


Fig. 4: Credential Ecosystem Blueprint

clarifies architectural trade-offs about what is stored or anchored, summarized in Fig. (4).

Lifecycle stages and trust logic

A trusted digital credential workflow in online education can be understood as a lifecycle connecting issuance, storage, presentation, verification, and ongoing validity, with **trust checkpoints** at each transition. Each checkpoint is intended to prevent specific breakdowns, including credentials created by unauthorized issuers (for example, an institution), credentials that are modified after issuance, presentations that disclose more than required, and verifications that reveal unnecessary information about the holder (the learner). These checkpoints are most robust when they use privacy-preserving authentication design patterns, particularly selective disclosure and strong binding between the credential and the intended holder.[14]

At issuance, trust begins by confirming the issuer's legitimacy and authority to issue the relevant credential type, and then by producing an integrity-protected credential record that can be independently validated later. Storage is then a continuity concern: the credential should remain accessible and verifiable even if learning platforms change, while keeping personal data under holder control where feasible. Presentation adds an explicit privacy and consent checkpoint, where the holder discloses only the attributes needed for a particular decision and avoids unnecessary exposure of academic history.[14]

Verification must then evaluate three elements together: the issuer is legitimate, the credential has not been altered, and the credential is valid at the time of checking. Ongoing validity, by contrast, depends on operational support for updates, corrections, expiration rules, and revocation signalling, allowing credentials to be invalidated when warranted without weakening the wider record system. Because verification is often performed at scale and under time constraints, these checkpoints should be achievable through **lightweight verification** steps that limit computation and network dependencies while preserving privacy guarantees.[14, 15]

System boundaries: blockchain linkage, off-chain data, and portability

Blockchain linked credential systems depend on a clear separation between public verification signals and private student records. In a privacy oriented

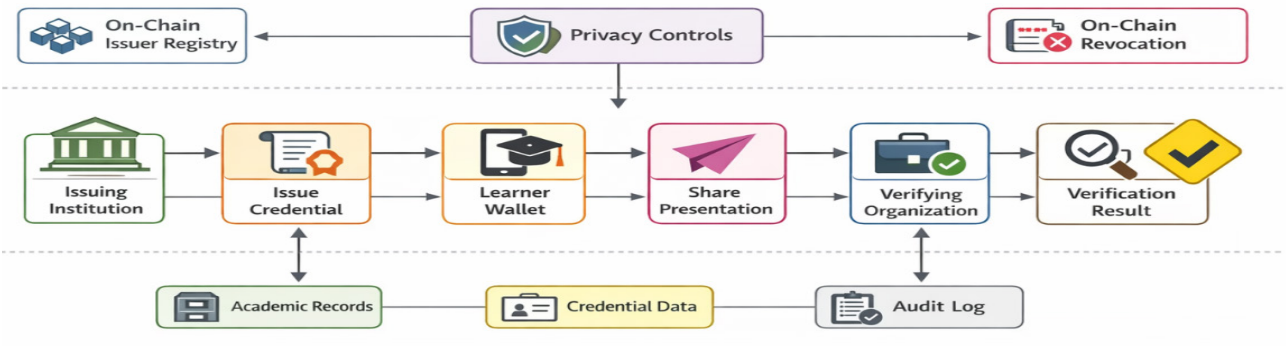


Fig. 5: On-chain vs off-chain data flow

design, only a minimal on chain anchor is committed to the ledger, while identifiable attributes remain off chain under privacy preserving access control,[16] as summarized in Fig. (5). To connect the public anchor to off chain metadata without revealing the metadata, the system stores a hash of that metadata, which supports later integrity checks, Eq. (1).

$$h = H(m) \tag{1}$$

Integrity verification then recomputes the hash from the off chain metadata and checks whether it matches the on chain anchor, Eq. (2).

$$IntegrityOK = 1[H(m) = h] \tag{2}$$

Portability and interoperability become salient when the same credential must be verified across learning platforms, registrars, and employers that use different data models and governance rules. In this setting, failed verifications are expected when a verifier cannot interpret, authorize, or validate the presented credential under its local rules. A portability summary therefore reports the fraction of attempted verifications that succeed across verifiers, Eq. (3).

$$PortabilityRate = \frac{N_{verified}}{N_{attempted}} \tag{3}$$

Data sharing can be strengthened by using permissioned chains that keep institutional control, together with proof techniques that disclose only what is required for verification, aligning cross system use with privacy.[16, 17]

Governance, Interoperability, and Implementation Logic

Operational viability of a blockchain-linked credential ecosystem depends, in practice, on aligning technical design with institutional decision rights, shared standards, and realistic adoption paths. The viability logic is summarized in Fig. (6). Interoperability requires consistent credential schemas, identifiers, and verification interfaces across issuers and verifiers. Governance must define issuance authority, procedures for updates and corrections, and accountability for revocation. Privacy choices should minimize disclosure while still enabling complete verification, so that participation remains acceptable to learners, institutions, and external evaluators.

Governance stack and standards alignment

Trusted digital credentialing in online education depends on a governance stack that links standards, institutional rules, and verification operations. In this framework, a credential is accepted only when issuer legitimacy, integrity, and revocation status are checked at the point of use. This requirement clarifies the need for clear authority, audit trails, and escalation paths for disputes and updates.[18] Security taxonomies and stated open challenges elaborate these requirements into concrete governance questions, while differentiating transparency from unlimited exposure.[18, 19]

Key trade-offs for implementing this stack are summarized in Tab. (4). Standards alignment supports cross-system compatibility, however it can limit local workflow customization, while explicit issuer holder

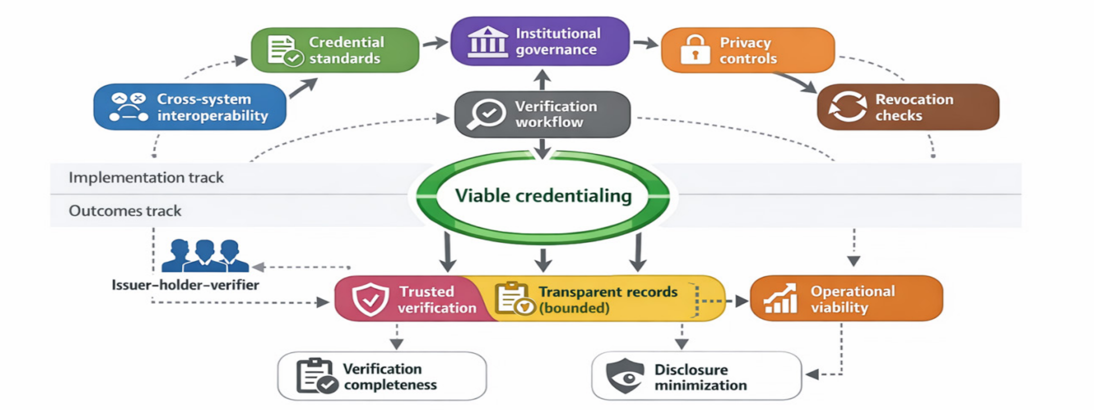


Fig. 6: Logic model for viable credentialing

Table 4: Standards and governance trade-offs

Design Choice	What It Prioritizes	What It Trades Off
Standards Alignment	Cross-system compatibility, smoother adoption across institutions	Less freedom to customize workflows; must fit institutional rules and shared formats
Issuer Holder Verifier Roles	Clear responsibility for issuing, holding, and checking credentials	More coordination work across organizations; role disputes must be governed
Privacy And Disclosure Minimization	Sharing only what is needed for a verification task	Reduced transparency for third parties; harder auditing without agreed access rules
Revocation And Correction	Accurate status over time, support for withdrawal and updates	Extra process and governance for revocation decisions and timely propagation to verifiers
On Chain vs Off Chain Handling	Practical system boundaries, avoid low-level cryptographic detail, keep workflows usable	Harder to explain and manage what is recorded where; governance needed to keep records consistent

verifier roles improve responsibility clarity at the cost of coordination across organizations. Privacy and disclosure minimization restrict what is shared for verification, which can reduce third-party visibility unless access rules are agreed. Revocation and correction keep credentials accurate over time, but they add decision processes and timely propagation duties, especially when responsibilities are split between on chain and off chain components.

Privacy, transparency limits, and revocation operations

Trusted online education credentials depend on transparency that is limited to what a verifier must learn to make a decision. In this framing, transparency is an information flow control problem, and the design goal is to disclose only the minimum data needed to assess issuer legitimacy, credential integrity, and revocation status, while keeping the remainder private.[20] Design choices that minimize disclosure across common verification needs are summarized in Tab. (5).

Privacy failures often concentrate in disclosure and proofing. Attempts to strengthen assurance can also create new sensitive data stores, and these tradeoffs are especially acute when verification designs accumulate identifiers that are difficult to revise after compromise.[20, 21] Trustworthy verification therefore depends on revocation and correction operations that are timely, auditable, and specific to the credential, so that a verifier can confirm current validity without learning unnecessary academic history. A bounded transparency stance treats revocation status as required evidence rather than optional metadata.[20]

Discussion and Implications

Applied to online education, the framework supports portable digital credentials that verifiers can validate without slow, manual transcript exchange, while institutions retain authority to issue, update, and revoke records. Verification is considered complete, and otherwise fails, unless issuer legitimacy, credential integrity, and non-revocation are jointly satisfied in Eq. (4).

$$VerifyComplete = IssuerOK \cdot IntegrityOK \cdot NotRevoked \tag{4}$$

Privacy and transparency are bounded by disclosing only what a check requires, as formalized by Eq. (5).

$$DisclosureMin = min\left(1, \frac{|A_{required}|}{|A_{disclosed}|}\right) \tag{5}$$

Table 5: Disclosure minimization design options

Verification Need	Minimum Disclosure	Privacy Note	What Must Still Hold
Issuer Legitimacy	Proof the issuer is legitimate (issuer identity needed for the check)	Limit shared issuer-related details to what the verifier needs for legitimacy	Must support trusted verification across institutions
Credential Integrity	Proof the credential has not been altered (integrity evidence needed for the check)	Share only what is needed to confirm integrity, not extra learner or program details	Must support a verifiable credential workflow
Revocation Status	Revocation status for the specific credential (revocation information needed for the check)	Reveal only revocation status needed for verification, avoid broader disclosure	Verification should include revocation as part of completeness
Verification Task Fit	Only the information needed for the specific verification task	Disclosure minimization means revealing only what is needed, not full academic records	Must balance privacy with realistic academic transparency limits

Table 6: Limitations, risks, and mitigations

Limitation Or Risk	Why It Matters	Mitigation In Framework
Blockchain-first framing	Reduces a credential ecosystem problem to a technology novelty	Start from credential workflow roles and lifecycle stages, keep low-level protocol detail out
Overstated transparency	Confuses auditability with unlimited access to learner data	Define transparency with limits, pair it with privacy controls and institutional rules
Weak revocation handling	Old or incorrect credentials can still appear valid	Treat revocation as part of verification and lifecycle, include revocation status checks
Poor interoperability	Credentials do not travel across institutions and systems	Use standards-aware reasoning and cross-system compatibility as a core design condition
Adoption and governance constraints	Institutional complexity can block deployment even when technology works	Make governance requirements explicit, align technology choices with institutional rules and practices

However, the framework does not address identity proofing or governance disputes.

Implications, limitations, and adaptation

The framework supports institutions and online learning platforms by treating credential trust as a workflow design problem. It clarifies issuer, holder, and verifier responsibilities, specifies what evidence must be checked at verification time, and separates learner data from audit signals. This framing can inform platform integration decisions, registrar operations, and procurement criteria by centering evaluation on interoperability, privacy safeguards, and lifecycle handling rather than on a ledger.

Key limitations and adoption risks are summarized in Tab. (6). The main failure modes are technology-first framing, overstated transparency, weak revocation, poor cross-system compatibility, and governance constraints. The framework is designed to address these by anchoring decisions in lifecycle stages, defining transparency with limits, treating revocation as mandatory during verification, using standards-aware interfaces, and aligning technical choices with institutional rules. As standards and governance evolve, the framework should be updated by revising these constraints rather than by adding speculative claims.

Conclusion

This study consolidates a standards-aware credential ecosystem model for online education in which blockchain linkage is treated as one element within a trust workflow. The model clarifies how issuer-holder-verifier roles connect across the credential lifecycle, and it differentiates verification as a combined check of issuer legitimacy, credential integrity, and current status, including cases of revocation and correction. Taken together, interoperability requirements and disclosure minimization situate transparency in auditable provenance and status rather than in exposing learner data. Overall, the model provides a practical basis for designing and evaluating trustworthy digital credential practice.

References

1. K. Jordan, “Initial trends in enrolment and completion of massive open online courses,” The International Review of Research in Open and Distributed Learning, vol. 15, no. 1, Jan. 2014, doi: 10.19173/irrodl.v15i1.1651.
2. H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and application of zero trust security: A brief survey,” Entropy, vol. 25, no. 12, pp. 1595-1595, Nov. 2023, doi: 10.3390/e25121595.
3. G. Akhison, “Towards a universal digital identity: A blockchain-based framework for borderless verification,” Frontiers in Blockchain, vol. 8, Nov. 2025, doi: 10.3389/fbloc.2025.1688287.
4. Zambrano-Ortiz, L. (2025). Decentralized Academic Credentials Using Blockchain Technology: A Systematic Review of Online Education Systems. International Journal on Research and Development - A Management Review, 14(1), 415-425.
5. G. Oestreicher-Singer and L. Zalmanson, “Content or community? A digital business strategy for content providers in the social Age1,” MIS Quarterly, vol. 37, no. 2, pp. 591-616, June 2013, doi: 10.25300/misq/2013/37.2.12.
6. P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, “Security and privacy of technologies in health information systems: A systematic literature review,” Computers, vol. 13, no. 2, pp. 41-41, Jan. 2024, doi: 10.3390/computers13020041.
7. M. T. Burrows, M. Abadi, and R. M. Needham, “A logic of authentication,” ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, Feb. 1990, doi: 10.1145/77648.77649.
8. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/tcsvt.2003.818349.
9. Ekanayake, E. (2025). Blockchain Applications for Secure Credential Verification in Digital Education Platforms: A Review Study. International Journal on Advanced Computer Engineering and Communication Technology, 14(1), 796-805.
10. Hugh, Q. (2024). Blockchain-Based Data Integrity Framework for Secure Cloud Storage Systems. Transactions on Internet Security, Cloud Services, and Distributed Applications, 8-14.
11. L. Liu et al., “BCCG: Blockchain-assisted cross-domain and group authentication protocol for

vehicle networks," IEEE Internet of Things Journal, vol. 12, no. 22, pp. 47844–47859, Aug. 2025, doi: 10.1109/jiot.2025.3603173.

12. B. Sule and S. Oruganti, "A conceptual framework for intelligent learning systems in microfinance education," International Journal of Recent Advances in Engineering and Technology, vol. 15, no. 1, pp. 79–88, 2026, Available: https://journals.mriindia.com/index.php/ijraet/article/view/1757
13. G. R. Blakley, "Safeguarding cryptographic keys," 1979 International Workshop on Managing Requirements Knowledge (MARK), pp. 313–318, June 1979, doi: 10.1109/mark.1979.8817296.
14. G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das, and Y. Park, "An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment," IEEE Access, vol. 11, pp. 26877–26892, Jan. 2023,doi: 10.1109/access.2023.3249116.
15. Nagamani, N. (2023). A comparative analysis of classical and quantum machine learning models for financial fraud detection. Computer Fraud & Security, 2023(12), 58-63. https://doi.org/10.52710/cfs.895
16. A. Alabdulatif, "Blockchain-based privacy-preserving authentication and access control model for e-health users," Information, vol. 16, no. 3, pp. 219–219, Mar. 2025, doi: 10.3390/info160 30219.
17. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8065–8073, Mar. 2022, doi: 10.1109/tii.2022.3161631.
18. N. Syed, S. W. A. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," IEEE Access, vol. 10, pp. 57143–57179, Jan. 2022, doi: 10.1109/access.2022.3174679.
19. Kingdon, C. C., & Luedke, R. G. (2025). Integrating Blockchain with Information Governance: A Multidisciplinary Framework for Academic Institutions. Bridge: Journal of Multidisciplinary Explorations, 1(2), 77-84.
20. Jadhav, K. D., Narayana, A., Chaudhari, L. B., Monisha J., Ambhore, V., & Shelke, G. C. (2026). AI-GENERATED LEARNING RESOURCES FOR CREATIVE FIELDS. *ShodhKosh: Journal of Visual and Performing Arts*, *7*(1s), 147–157. https://doi.org/10.29121/shodhkosh.v7.i1s.2025.7080
21. Belhocine, I. (2025). Blockchain-Based Credentialing in Online Education: A Review of Trust, Verification, and Academic Transparency Mechanisms. International Journal of Recent Advances in Engineering and Technology, 14(1), 235–244.
22. N. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication Surendar, A. (2025). Sustainable Digital Governance in Academic Institutions Using Blockchain-Enabled Infrastructure. Journal of Smart Infrastructure and Environmental Sustainability, 2(2), 26-32.
23.Asadullah, M., Sinha, D., Kumar, S., Kumari, R., Kaur, A., & Kaur, J. (2026). Artificial Intelligence in Personalised Learning System. International Journal on Research and Development - A Management Review, 15(1), 112–120.