The OCEM Journal of
Management, Technology & Social Sciences

Received: May 02, 2026 | Revised: May 13, 2026 | Accepted: May 25, 2026 | Published: July 10, 2026

DOI: 10.3126/ocemjmtss.v5i2.1014 **Paper Type: Research Article**

Implementing Blockchain in Higher Education: Technical Architecture, Administrative Challenges, and Policy Directions for Nepal and Least Developed Countries

Dipendra Silwal[1]*, Dharma Raj Upreti[2]
[1]Faculty of Computer Application, Oxford College of Engineering & Management, Gaindakot
[2]Faculty of Business Administration, Oxford College of Engineering & Management, Gaindakot
*Correspondence email: dipendrraaa@gmail.com

Volume 5, Issue 2

ISSN Print:2705-4845

ISSN Online:2705-4845

Abstract

This systematic literature review investigates the implementation of blockchain technology in higher education for academic credential issuance, record verification, and trust-building across institutions, with a focus on Nepal and similar least-developed-country contexts. This review is organised based on three research questions, which are proposed technical architecture, administrative and infrastructural barriers to adoption, and policy requirements for secure and credible implementation. Reliable, published, and influential sources were identified through a PRISMA-inspired search and screening protocol, including peer-reviewed journal articles, indexed conference proceedings, and official legal and standards documents. A total of two hundred and fourteen (N = 214) papers were screened, and seventeen (n = 17) core sources were included for qualitative synthesis.

The results show that blockchain-based credentialing is technically mature at the prototype level.They further show that many proposed systems have layered architecture consisting of an application interface, an identity and credential layer, a blockchain ledger, and off-chain storage. Empirical findings shows that blockchain success depends not only on application but also on legal recognition, institutional readiness, interoperability, privacy protection, key management, and employer-side verification. However, in Nepal's case, the review argues that the direct implementation within the country may be early. A strong policy approach is needed, beginning with legal recognition of digital and blockchain-verifiable credentials, adoption of W3C Verifiable Credentials and Decentralised Identifiers, small university pilots, privacy impact assessment, onboarding of public-sector verifiers, and planning for failed or abandoned systems. The review concludes that blockchain can support academic credential verification in Nepal and similar contexts, but it needs to be viewed as a long-term institutional infrastructure.

Keywords: *academic credentials, blockchain, digital certificates, higher education, least developed countries, Nepal, policy*

How to cite this paper:
Silwal, D., & Upreti, D.R. (2026). Implementing Blockchain in Higher Education: Technical Architecture, Administrative Challenges, and Policy Directions for Nepal and Least Developed Countries. *The OCEM Journal of Management, Technology & Social Sciences*, *5*(2), 178-188.

Introduction

Higher education systems are increasingly operating in a globalised environment in which students seek employment, migration, further education, and professional recognition beyond their home countries. Academic credentials serve not only as educational documents but also as cross-border instruments of trust (Alammary et al., 2019). Traditional credential verification systems largely rely on registrar offices, paper certificates, sealed envelopes, manual emails, and institutional databases that may not be interoperable across universities or countries, which lead to delays, increased administrative workload, and potential opportunities for document tampering or fraudulent claims. Blockchain has been proposed as a solution because it can create a tamper-evident record of credential issuance and make verification possible without repeated communication with the issuing institution (Giri, 2018).

Early education-focused blockchain research argued that distributed ledgers could support persistent educational records and reputational evidence beyond conventional transcripts (Sharples & Domingue, 2016). Later work extended this idea to higher education credits, digital certificates, lifelong learning records, and secure educational record sharing (Jirgensons & Kapenieks, 2018; Ocheja et al., 2019; Turkanović et al., 2018), which is highly relevant for Nepal and other LDCs. Nepal remains an LDC on the United Nations list and is scheduled to graduate on 24 November 2026, but its higher education governance and digital public infrastructure remain uneven.

Nepal's Electronic Transactions Act recognises electronic records and digital signatures but does not provide a dedicated legal framework for distributed-ledger credentials (Government of Nepal, 2008). Nepal's Digital Nepal Framework also emphasises digital transformation, but implementing secure, interoperable credentials will require technical standards, institutional capacity, and clear governance beyond general digitalisation objectives (Giri, 2018). This review, therefore, takes a cautious position. It does not assume that blockchain automatically solves credential fraud, administrative delay, or trust deficits. Instead, it asks when blockchain-based credential systems are technically feasible, administratively manageable, legally recognisable, and contextually appropriate for resource-constrained higher education systems (Alangari et al., 2022).

Review Questions

This review was guided by the research questions document supplied for this project.

RQ1:What technical architectures are proposed for implementing blockchain technology in higher education institutions in Nepal and comparable LDC contexts?

RQ2:What administrative, organisational, and infrastructural challenges are associated with adopting blockchain for higher education credentialing and record verification in LDCs?

RQ:3What policy directions and regulatory frameworks are recommended to facilitate secure and effective blockchain integration in Nepalese higher education?

Methodology

This review followed a PRISMA (2020)-informed design, which is widely used to make systematic reviews more transparent in the identification, screening, and inclusion of records (Page et al., 2021). The screening record used for this paper identified two hundred fourteen (N = 214) records through database and citation-network searches. After removing thirty-seven duplicates, one hundred seventy-six (N = 176) records were screened based on the title and abstract. From one hundred thirty-nine (N = 139) records were excluded because they were off-topic, non-peer-reviewed, non-English, or insufficiently relevant to higher education credentialing. Forty-five full-text articles were assessed for eligibility; twenty-eight were excluded because they lacked sufficient empirical, design-science, architectural, or policy relevance, and seventeen core sources were retained for final qualitative synthesis, which included counts corresponding to the sources mapped; background, methodological, and contextual references were cited separately where

needed (see Table 2).

The search logic combined terms related to blockchain, distributed ledger technology, higher education, digital credentials, certificates, transcripts, verification, architecture, governance, policy, Nepal, developing countries, and least developed countries. Although the supplied protocol initially emphasised the period 2021-2026, foundational studies published between 2016 and 2020 were retained because the most influential blockchain-in-education architectures appeared before 2021. Excluding these early studies would distort the history and technical development of the field.

The PRISMA flow diagram for study selection presents the corrected screening record for this PRISMA-informed review. Two hundred and fourteen records identified, thirty-eight duplicates removed, one hundred and seventy-six records screened, forty-five full texts assessed, twenty-eight full texts excluded, and seventeen core sources retained for qualitative synthesis (see Figure 1).

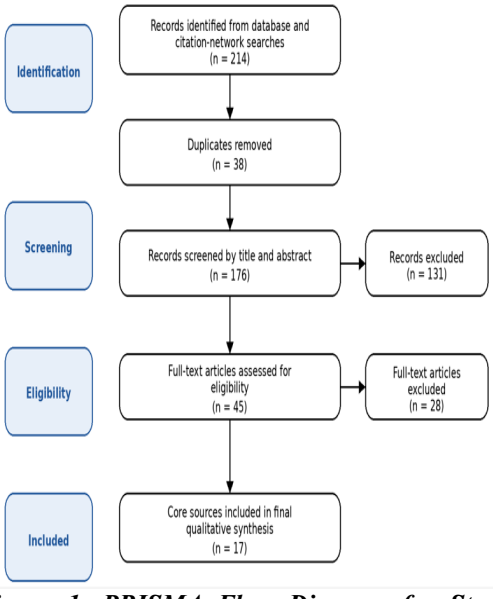

Figure 1. PRISMA Flow Diagram for Study Selection (Page et al., 2021)

The review reports the corrected screening record used in this PRISMA-informed review: two hundred fourteen 214 records identified, thirty-eight duplicates removed, one hundred seventy-six records screened, forty-eight full texts assessed, twenty-eight full texts excluded, and seventeen core sources retained for qualitative synthesis (see Figure 1).

Table 1. Search and Screening Protocol

Element	Decision Applied in this Review
Primary topic	Blockchain or distributed ledger technology applied to higher education credentials, transcripts, academic records, lifelong learning records, or education administration.
Publication status	Published journal articles, indexed conference proceedings, reputable books/chapters, official standards, and official government or intergovernmental documents.
Exclusion rule	Unpublished preprints, unverifiable papers, duplicate secondary claims, weak non-peer-reviewed articles, and papers not directly connected to education records or implementation.
Contextual filter	Studies with direct implications for Nepal, LDCs, developing countries, resource-constrained institutions, or public-sector digital governance were prioritised.
Citation rule	APA 7 author-date in-text citations; references restricted to genuine published or official sources.

The protocol is PRISMA-informed; screening counts used in this article were records identified (n = 214), duplicates removed (n = 38), records screened (n = 176), records excluded after title/abstract screening (n = 131), full-text articles assessed (n = 45), full-text articles excluded (n = 28), and core sources retained for qualitative synthesis (n = 17).

Thematic Synthesis of Literature

Three broad bodies of literature were included in the core synthesis shown in Table 2. The first collection consists of conceptual and review papers that map the educational uses, benefits, and risks of blockchain (Acharya et al. 2025; Alammary et al., 2019; Bhaskar, Tiwari & Joshi, 2021; Chen et al., 2018). The second contains design-science and prototype studies that suggest systems for credits, certificates, records, or learning histories (Arenas & Fernandez, 2018; Gräether et al., 2018; Li et al., 2019; Ocheja et al., 2019; Turkanović et al., 2018). The third includes sources related to adoption, governance, privacy, and policy that

clarify institutional, regulatory, and user-side issues (Bhattarai, 2021; Finck, 2018; Rooksby & Dimitrov, 2019; Ullah et al., 2021; W3C, 2022, 2025).

Table 2. Core Literature Streams Included in the Review

Theme	Included Published/ Official Sources	Main Contribution
Education blockchain reviews	Alammary et al. (2019). Bhaskar et al. (2021); Chen et al. (2018)	Establish the range of blockchain applications in education and identify credentialing as one of the most developed use cases.
Credential and certificate prototypes	Arenas and Fernandez (2018). Gräther et al. (2018); Turkanović et al. (2018)	Demonstrate technical feasibility of verifiable credentials, permissioned ledgers, and higher education credit systems.
Secure record storage and sharing	Li et al. (2019); Ocheja et al. (2019)	Show the value of off-chain storage, smart contracts, and lifelong record management.
Institutional adoption and trust	Rooksby and Dimitrov (2019). Ullah et al. (2021)	Show that adoption depends on institutional values, perceived usefulness, compatibility, and governance.
Privacy and legal constraints	Finck (2018); W3C (2022, 2025)	Clarify the conflict between immutability and data protection, and support credential interoperability through DID and VC standards.
Nepalese context	Bhattarai (2021); Government of Nepal (2008, 2019); UGC Nepal (2024), Acharya et al. (2025)	Ground the review in Nepalese ICT policy, legal recognition, and higher education governance constraints.

Technical Architecture for Blockchain in Higher Education

The most defensible architecture for blockchain-based academic credentialing is not to place full certificates or transcripts directly on-chain. Instead, the issuing university creates a credential, digitally signs it, stores the full document in a controlled off-chain repository, and writes only a cryptographic hash or proof of issuance to a blockchain ledger. A verifier later checks whether the presented credential produces the same hash as the record anchored on the chain. This design maintains integrity while avoiding excessive on-chain storage and reducing exposure of personal data (Li et al., 2019). Variants of this architecture are reported in the literature. EduCTX proposed a blockchain-based higher-education credit platform aligned with the European Credit Transfer and Accumulation System, demonstrating that credits could be represented in a distributed environment (Turkanović et al., 2018).

Credence Ledger proposed a permissioned blockchain model for verifiable academic credentials, where compact proofs are stored rather than full credential documents (Arenas & Fernandez, 2018). Blockchain for Education: Lifelong Learning Passport proposed a practical platform for issuing, validating, and sharing certificates through blockchain-based authority management (Gräther et al., 2018). For Nepal and LDCs, the most appropriate architecture is therefore a layered, permissioned, and standards-based model. Public permissionless chains offer high openness but have fluctuating transaction costs, opaque governance, and privacy risks. Fully private chains offer institutional control but may undermine cross-border trust (Acharya et al., 2025). A permissioned consortium model, governed by universities and a public education authority, offers a more realistic balance for a national higher education system (see Figure 2).

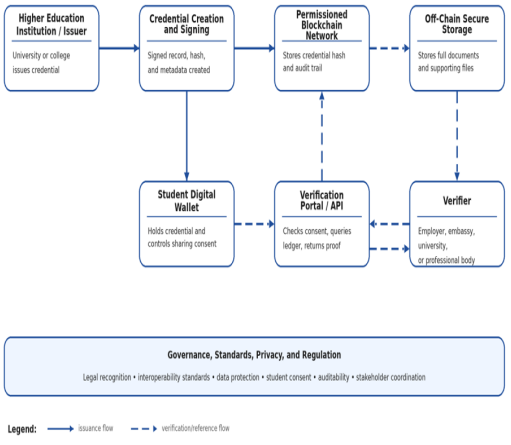

Figure 2. Proposed Blockchain-based Academic Credential Verification Architecture for Nepal and LDCs

Table 3. Recommended Layered Architecture for Nepal and LDC Higher Education

Layer	Function	Recommended Design for Nepal/LDCs	Main Risk
Application layer	Issuer portal, verifier portal, student credential view, QR-code interface	Web-based portal plus QR-verifiable credential; avoid assuming all students can use advanced digital wallets.	Low employer or student use if interfaces are difficult or unknown.
Identity and credential layer	Links credentials to the student and institution; supports selective disclosure.	W3C Verifiable Credentials and Decentralised Identifiers; institutional identity registry for issuers.	Identity mismatch, lost keys, weak consent, or poor user literacy.
Ledger layer	Tamper-evident record of issuance, revocation, and verification events	Permissioned consortium chain governed by universities, UGC, and the Ministry of Education or equivalent authority.	Governance capture, node downtime, and unclear dispute handling.
Storage layer	Stores a full transcript/ certificate, while blockchain stores only a hash/proof	Encrypted off-chain storage with institutional backup and hash anchoring.	Record loss if storage governance is weak despite a valid on-chain hash.
Governance layer	Defines legal recognition, roles, audit, privacy, and continuity	National credential policy, data protection impact assessment, key escrow, and continuity protocol.	Technically, the working system remains legally or administratively unused.

Source: (Tiwari, 1977)

Permissioned Versus Permissionless Design

A central architectural debate concerns whether higher education should use public permissionless blockchains or permissioned networks. Public chains are attractive because any verifier can independently inspect the ledger. However, public systems may expose metadata, depend on external network economics, and create long-term governance uncertainty. Permissioned systems reduce transaction costs and enable known institutions to curate validator membership, but they reintroduce reliance on the consortium's governance. The choice is not just technical but defines whether the system values global openness or institutional accountability. Literature is generally biased toward permission or consortium models for real higher-education credentialing. Credence Ledger's permissioned model is especially relevant because academic credential verification requires known issuers, regulated authorities, and controlled write access (Arenas & Fernandez, 2018). A permissioned model would also associate better with public-sector accountability and phased implementation in Nepal (see Table 3).

Identity, Privacy, and Interoperability

Identity is the weak point of many blockchain credential systems. A blockchain can prove

that a credential was issued and not altered. However, it does not automatically prove that the person presenting it is the rightful holder. W3C Decentralised Identifiers and Verifiable Credentials offer a standards-based approach for representing issuers, holders, and verifiers and for enabling machine-verifiable credentials (World Wide Web Consortium, 2022, 2025). DID-based systems for Nepal and LDCs cannot assume universal smartphone ownership, reliable internet, or high digital literacy. Privacy matters as much. Finck (2018) explains that blockchains create difficult questions for data protection because immutability conflicts with rights to modification, erasure, and purpose limitation. For higher education, the practical implication is clear: personally identifiable student data should not be stored directly on the chain. The better design is to store only a hash or proof on-chain and keep the full credential in a controlled, revocable, access-managed repository.

Administrative, Organisational, and Infrastructural Challenges

The main barrier to implementation is not the absence of blockchain prototypes. The literature already contains multiple working or conceptual systems. The more serious challenge is the gap between technical demonstration and institutional deployment. Rooksby and Dimitrov (2019) demonstrated that blockchain systems can create tensions with university procedures, institutional boundaries, and traditional trust relationships. Ullah et al. (2021) further revealed that adoption depends on perceived usefulness, compatibility, and institutional conditions rather than technical novelty alone. In Nepal, policy and infrastructure conditions further widen this gap. Bhattarai (2021) argues that policy gaps, uneven readiness, and the need for a stronger enabling environment are obstacles to Nepal's ICT development. Higher education credentialing also involves multiple actors: universities, affiliated colleges, examination boards, UGC, ministries, students, employers, professional councils, foreign credential evaluators, and recruitment agencies. A blockchain credential is valuable only if these actors trust, recognise, and use it (see Table 4).

Table 4. Administrative and Infrastructural Challenges

Challenge	Why It Matters	Implication for Nepal/LDCs
Legal recognition	A technically valid blockchain credential may still be rejected if the law recognises only paper or conventional digital signatures.	Amend or interpret existing electronic transaction laws to recognise digitally signed and blockchain-verifiable credentials.
Institutional capacity	Universities need trained staff for issuance, revocation, key management, audits, and user support.	Capacity-building budgets must be included from the beginning, not added after software procurement.
Interoperability	Different universities may create incompatible credential formats.	Adopt national W3C VC/DID-based credential schemas before large pilots.
Privacy and consent	Student data are sensitive and long-lived; immutable storage may violate privacy expectations.	Store personal records off-chain; conduct data protection impact assessments; obtain informed consent.
Verifier adoption	Employers and government offices must know how to verify credentials.	The pilot must include employers and public-sector HR offices, not only universities.
Infrastructure reliability	Nodes and portals require stable electricity, internet access, backup power, and cybersecurity controls.	Use hub-and-spoke infrastructure, offline queues, backups, and disaster recovery.
Continuity risk	Students may be harmed if a platform is abandoned or keys are lost.	Create escrow, migration, and continuity rules before issuing real credentials.

Policy Directions for Nepal and LDCs

Policy should begin with the problem to be solved, not with technology. If the main problem is slow, costly verification, blockchain is useful only when verifiers can verify credentials quickly. If the main problem is credential fraud, blockchain helps only if the first issuance is accurate and the issuer keys are protected. If the main problem is cross-border

portability, national implementation must adhere to interoperable standards rather than to isolated institutional software (Acharya et al., 2025) . For Nepal, the Electronic Transactions Act marks the beginning of electronic records and digital signatures. However, it needs to be extended or supplemented to cover blockchain-verifiable credentials, recognised issuers, revocation, evidentiary value, dispute resolution, and the role of public authorities (Government of Nepal, 2008). The Digital Nepal Framework provides a broader direction for digital transformation. However, higher education requires a specific national framework for credential governance (Giri, 2018).

Five-phase roadmap of blockchain adoption in higher education in Nepal (see Figure 3). The roadmap is consistent with the staged policy actions presented (see Table 5). It highlights the legal basis, institutional readiness, controlled pilot testing, privacy assurance, and Scale and regional recognition (see Table 5).

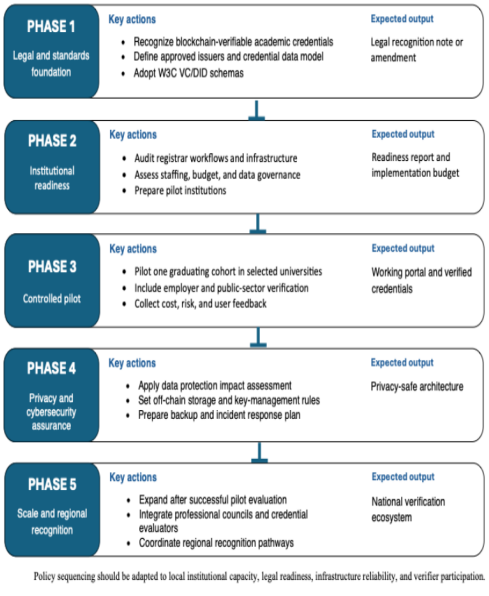

Figure 3. Five-phase Policy Roadmap for Blockchain Implementation in Nepalese Higher Education

The roadmap aligns with the staged policy actions and emphasises legal foundation, institutional readiness, controlled pilot testing, privacy assurance, and scale-up (see Table 5).

Table 5. Staged Policy Roadmap for Nepal

Challenge	Why It Matters	Implication for Nepal/LDCs
Legal recognition	A technically valid blockchain credential may still be rejected if the law recognises only paper or conventional digital signatures.	Amend or interpret existing electronic transaction laws to recognize digitally signed and blockchain-verifiable credentials.
Institutional capacity	Universities need trained staff for issuance, revocation, key management, audits, and user support.	Capacity-building budgets must be included from the beginning, not added after software procurement.
Interoperability	Different universities may create incompatible credential formats.	Adopt national W3C VC/DID-based credential schemas before large pilots.
Privacy and consent	Student data are sensitive and long-lived; immutable storage may violate privacy expectations.	Store personal records off-chain; conduct data protection impact assessments; obtain informed consent.
Verifier adoption	Employers and government offices must know how to verify credentials.	The pilot must include employers and public-sector HR offices, not only universities.
Infrastructure reliability	Nodes and portals require stable electricity, internet access, backup power, and cybersecurity controls.	Use hub-and-spoke infrastructure, offline queues, backups, and disaster recovery.
Continuity risk	Students may be harmed if a platform is abandoned or keys are lost.	Create escrow, migration, and continuity rules before issuing real credentials.

The roadmap is intentionally phased because legal recognition and verifier participation are preconditions for meaningful adoption.

Discussion

This systematic literature review demonstrates that blockchain technology has progressed beyond a purely conceptual innovation and has reached a level of technical maturity suitable for academic credential management. Across the reviewed

studies, there is broad agreement that blockchain can enhance the integrity, authenticity, and traceability of academic credentials by creating tamper-evident records that enable efficient verification without continuous reliance on issuing institutions. These findings are consistent with earlier studies that identified credential management as one of the most mature educational applications of blockchain technology (Sharples & Domingue, 2016; Alammary et al., 2019; Bhaskar et al., 2021). However, the review also reveals that technical feasibility alone is insufficient for successful implementation. Rather than representing a technological problem, blockchain adoption in higher education has increasingly become an institutional, legal, and governance challenge.

The review further indicates that a layered architecture comprising an application interface, an identity and credential management layer, a permissioned blockchain ledger, and secure off-chain storage represents the most appropriate design for higher education institutions. This finding reinforces existing architectural studies that advocate storing only cryptographic proofs on the blockchain while maintaining complete academic records in controlled repositories to balance security, privacy, and scalability. The preference for permissioned consortium blockchains also reflects the governance requirements of higher education, where credential issuance depends on trusted institutions, regulatory oversight, and clearly defined responsibilities rather than unrestricted public participation. Consequently, blockchain should be viewed as a complementary trust infrastructure integrated with existing university information systems rather than as a replacement for them.

One of the most important findings of this review is that institutional readiness constitutes a greater barrier to implementation than technological readiness. Although several blockchain-based credentialing prototypes have demonstrated technical viability, their transition into operational university systems remains limited. Successful implementation requires institutional commitment, skilled personnel, governance mechanisms, cybersecurity capacity, sustainable funding, and coordinated participation among universities, accreditation bodies, employers, and government agencies. This finding extends previous research by demonstrating that stakeholder trust and organisational capability are equally as important as technological innovation in determining implementation success. In resource-constrained environments such as Nepal, these institutional requirements become even more significant because digital transformation initiatives often progress more slowly than technological development.

The review also highlights the importance of legal recognition and interoperability. Existing legal frameworks in Nepal recognise electronic records and digital signatures but provide limited guidance regarding blockchain-verifiable academic credentials, decentralised identity management, credential revocation, or evidentiary standards. Without legal certainty, blockchain-generated credentials may fail to achieve widespread acceptance despite their technical reliability. Similarly, interoperability standards such as W3C Verifiable Credentials and Decentralised Identifiers emerge as essential prerequisites for cross-institutional and international recognition. These findings suggest that blockchain implementation should be considered a governance reform as much as a technological innovation.

Privacy and data protection remain critical considerations throughout the literature. Although blockchain provides immutability and transparency, these characteristics may conflict with privacy principles and individuals' rights to control personal information. The reviewed studies consistently recommend storing personally identifiable information off-chain while recording only on-chain cryptographic hashes. This hybrid architecture provides an effective balance between data integrity and regulatory compliance and is particularly relevant for countries seeking to strengthen digital governance while protecting student privacy.

From a theoretical perspective, this review contributes to the growing literature on blockchain adoption in higher education by shifting attention

from technological capability to institutional implementation. Existing research has predominantly focused on developing technical architectures and proof-of-concept systems. In contrast, this review demonstrates that sustainable adoption depends on the interaction between technology, governance, institutional capacity, legal frameworks, interoperability standards, and stakeholder acceptance. Accordingly, blockchain should be conceptualised as a socio-technical infrastructure whose effectiveness depends on coordinated institutional and policy arrangements rather than on technological innovation alone.

The review also provides important practical implications for Nepal and other least-developed countries. Rather than pursuing nationwide implementation immediately, policymakers should adopt a phased strategy beginning with legal reforms, development of national interoperability standards, institutional capacity building, and carefully evaluated pilot projects. Such an incremental approach reduces implementation risks while allowing universities and regulatory agencies to develop the organisational capabilities necessary for long-term sustainability. Future research should therefore move beyond prototype development towards empirical evaluation of pilot implementations, longitudinal assessment of institutional outcomes, governance effectiveness, user acceptance, and cross-border interoperability in developing-country contexts.

Research Gaps

Though existing studies demonstrate the technical feasibility of blockchain-based academic credential systems, most remain limited to prototype development and conceptual frameworks. Empirical evidence on large-scale institutional implementation, long-term governance and cost-effectiveness is limited, especially in least developed countries (LDCs). Furthermore, there is a lack of research on legal recognition, stakeholder adoption, interoperability, and the policy frameworks needed for sustainable deployment in contexts such as Nepal. These gaps underline the need for context-specific studies that integrate technical architecture with institutional readiness, regulatory support, and practical implementation strategies.

Conclusion

This systematic literature review examined the implementation of blockchain technology for academic credential issuance, verification, and institutional trust in higher education, with particular attention to Nepal and comparable least-developed-country contexts. The evidence indicates that blockchain technology has reached a considerable level of technical maturity for credential verification, with most proposed systems converging on layered architectures that combine permissioned blockchain networks, decentralised identity management, and secure off-chain storage. These architectural approaches provide a practical foundation for improving credential authenticity, reducing verification costs, and strengthening trust among educational institutions, employers, and regulatory authorities.

However, the review demonstrates that technological maturity alone does not ensure successful implementation. The principal barriers are institutional rather than technical, including inadequate legal recognition, limited governance capacity, insufficient interoperability standards, cybersecurity concerns, privacy protection, stakeholder acceptance, and organisational readiness. These findings indicate that blockchain should not be viewed as a stand-alone technological solution but rather as part of a broader institutional transformation that requires coordinated legal, administrative, and policy reforms.

The study makes an important theoretical contribution by extending current understanding of blockchain adoption beyond technical design toward a socio-technical governance perspective. It demonstrates that successful implementation depends on the interaction between technological architecture, institutional capability, legal legitimacy, and stakeholder trust. This integrated perspective provides a more comprehensive framework for future research on blockchain-enabled public digital infrastructure in higher education.

From a policy perspective, the review recommends a phased implementation strategy for Nepal

beginning with legal recognition of blockchain-verifiable credentials, adoption of internationally recognised interoperability standards such as W3C Verifiable Credentials and Decentralised Identifiers, institutional capacity development, pilot implementation in selected universities, and continuous evaluation before national deployment. Such a staged approach would minimise implementation risks while strengthening institutional confidence and public trust.

Although this review provides a comprehensive synthesis of the existing literature, its conclusions are limited by the relatively small number of empirical implementation studies, particularly in least-developed countries. Future research should therefore focus on longitudinal evaluations of blockchain pilot projects, comparative studies across developing economies, governance and regulatory effectiveness, cost-benefit analysis, user acceptance, and interoperability across international higher education systems. Addressing these research gaps will provide stronger evidence to guide policymakers and universities seeking to modernise academic credential management through blockchain technology.

References

Acharya, P., Sapkota, B., Thokar, B., & Dawadi, B. R. (2025). Streamlining the digital identity ecosystem in Nepal: A private blockchain approach. *International Journal on Engineering Technology and Infrastructure Development, 2*(1), 274–283. https://doi.org/10.3126/injet-indev.v2i1.82539

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences, 9*(12), Article 2400. https://doi.org/10.3390/app9122400

Alangari, S., Alshahrani, S. M., Khan, N. A., Alghamdi, A. A., Almalki, J., & Al Shehri, W. (2022). Developing a blockchain-based, digitally secured model for the educational sector in Saudi Arabia toward digital transformation. *PeerJ Computer Science, 8*, Article e1120. https://doi.org/10.7717/peerj-cs.1120

Arenas, R., & Fernandez, P. (2018). CredenceLedger: A permissioned blockchain for verifiable academic credentials. *In 2018, IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICE.2018.8436324

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2021). Blockchain in education management: Present and future applications. *Interactive Technology and Smart Education, 18*(1), 1–17. https://doi.org/10.1108/ITSE-07-2020-0102

Bhattarai, M. K. (2021). Information and communication technology scenario of Nepal: Assessing policy environment and challenges. *Nepal Public Policy Review, 1*(1), 201–211. https://doi.org/10.3126/nppr.v1i1.43443

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics, 36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments, 5*, Article 1. https://doi.org/10.1186/s40561-017-0050-x

Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review, 4*(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6

Giri, S. (2018). Dimensions of the digital Nepal framework and an appropriate roadmap. *International Journal of Science and Research (IJSR), 9*(1), 719–724.

Government of Nepal. (2008). The Electronic Transactions Act, 2063 (2008). Nepal Law Commission.

Government of Nepal, Ministry of Communication and Information Technology. (2019). Digital Nepal Framework.

Gräther, W., Kolvenbach, S., Ruland, R., Schütte,

J., Torres, C., & Wendland, F. (2018). Blockchain for education: Lifelong learning passport. *In Proceedings of the 1st ERCIM Blockchain Workshop 2018*. https://doi.org/10.18420/blockchain2018_07

Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the future of digital learning, credential assessment, and management. *Journal of Teacher Education for Sustainability, 20*(1), 145–156. https://doi.org/10.2478/jtes-2018-0009

Li, H., Han, D., Li, K.-C., & Castiglione, A. (2019). EduRSS: A blockchain-based educational records secure storage and sharing scheme. *IEEE Access, 7*, 179273–179289. https://doi.org/10.1109/ACCESS.2019.2956157

Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning, 14*, Article 4. https://doi.org/10.1186/s41039-019-0097-0

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

Rooksby, J., & Dimitrov, K. (2019). Trustless education? A blockchain system for university grades. *Ubiquity: The Journal of Pervasive Media, 6*(1), 83–88. https://doi.org/10.1386/ubiq_00010_1

Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation, and reward. *In K. Verbert, M. Sharples, & T. Klobučar (Eds.), Adaptive and adaptable learning: EC-TEL 2016 (Lecture Notes in Computer Science, Vol. 9891*, pp. 490–496). Springer. https://doi.org/10.1007/978-3-319-45153-4_48

Tiwari, S. R. (1977). *Architectural education in Nepal.* USA, University of Hawai'i at Manoa.

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

Ullah, N., Al-Rahmi, W. M., Alzahrani, A. I., Alfarraj, O., & Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments. *Sustainability, 13*(4), Article 1801. https://doi.org/10.3390/su13041801

University Grants Commission Nepal. (2024). *Education Management Information System: Report on Higher Education 2023/24*. University Grants Commission.

World Wide Web Consortium. (2022). *Decentralized identifiers (DIDs) v1.0: Core architecture, data model, and representations*. https://www.w3.org/TR/did-core/

World Wide Web Consortium. (2025). *Verifiable credentials data model v2.0.* https://www.w3.org/TR/vc-data-model-2.0/