Trends and Reviews of Technological Engineering in Education
Vol. 3, No. 2 (2025) | ISSN 3071-2211 | Open Access

REVIEW ARTICLE

Smart Contract-Enabled Micro-Credentialing for Competency-Based E-Learning: Architecture, Empirical Analysis, and Design Guidelines

Lianliang Wei[1,*], Mohammed Al-Harthi[1], Ruiwei Chen[1]
[1] School of Educational Technology, Beijing Normal University, Beijing 100875, China
* Correspondence: lianliang.wei@bnu.edu.cn

Article Information

Received	14 December 2024
Revised	10 March 2025
Accepted	22 June 2025
Published Online	30 June 2025

Abstract

Competency-Based Education (CBE) demands credential systems that are granular, portable, tamper-evident, and continuously updatable — requirements that traditional Learning Management Systems (LMS) cannot satisfy. Smart contract technology, deployed on permissioned blockchain networks, offers a programmable trust layer capable of automating micro-credential issuance, enforcing competency prerequisites, and enabling employer-facing verifiable presentations without institutional intermediaries. This article presents a comprehensive review and empirical analysis of smart contract-enabled micro-credentialing systems, synthesising 76 peer-reviewed studies published between 2018 and 2025 through a PRISMA-guided Systematic Literature Review (SLR). We propose a five-layer reference architecture integrating Hyperledger Fabric chaincode, W3C Verifiable Credentials, Decentralised Identifiers (DIDs), and IPFS-based hybrid storage. Empirical benchmarking across five blockchain platforms reveals that Hyperledger Fabric achieves optimal throughput (3,500 TPS) and lowest latency (0.5 s average) for educational workloads. A multi-criteria evaluation covering security, privacy, scalability, GDPR compliance, and interoperability demonstrates that SSI-anchored architectures outperform both public blockchain and centralised LMS alternatives across seven dimensions. Critical barriers — including oracle security gaps, GDPR/FERPA regulatory conflicts, smart contract auditability, and digital equity concerns — are systematically analysed, and a five-phase institutional implementation roadmap is proposed. This work provides the most architecturally complete and empirically grounded blueprint to date for practitioners designing next-generation, blockchain-secured competency credential ecosystems.

Keywords: Smart Contracts; Micro-Credentialing; Competency-Based Education; Blockchain; Hyperledger Fabric; W3C Verifiable Credentials; Decentralised Identity; GDPR.

1. Introduction

The global shift toward competency-based education (CBE) has fundamentally redefined the unit of educational value. Rather than the credit hour — a proxy measure rooted in seat-time industrialism — CBE frames learning outcomes in terms of demonstrable, assessable competencies [1], [2], [47]. This paradigm shift is reflected in institutional policy across multiple continents: the European Qualifications Framework (EQF), the Australian Qualifications Framework (AQF), and the United States Department of Education's CBE Direct Assessment programmes collectively represent credentialing reform at national scale [3], [58], [66]. Concurrent with this policy evolution, the labour market has accelerated its demand for granular, verifiable skill attestations. LinkedIn's 2024 Workforce Report estimates that 68% of

How to cite: Petrova et al. (2023). Artificial Intelligence for Personalized Learning Analytics: Adaptive Pathways, Student Modeling, and Educational Equity. TRTEE, 3(2), 1–27. https://doi.org/10.63646/trtee.2025.030201

hiring managers now weight skill-specific micro-credentials alongside, or ahead of, traditional four-year degrees for technical roles — a figure that was below 30% in 2018 [60], [61].

Yet the credential infrastructure supporting this transition remains archaic. Despite decades of digital transformation in education, the dominant credential artefact — the paper or PDF diploma — remains inherently vulnerable to forgery, institutionally siloed, and incapable of representing the micro-granular competency distinctions that CBE demands [4], [9], [21]. A 2023 study by the Association of American Collegiate Registrars and Admissions Officers (AACRAO) found that 36% of surveyed employers had encountered fraudulent academic credentials in the preceding two years, with remediation costs averaging USD 8,400 per incident [60]. At a global scale, diploma fraud is estimated to cost educational institutions and employers USD 1.2 billion annually in verification overhead and reputational remediation [61], [79].

Smart contract technology, deployed on permissioned blockchain networks, addresses these structural vulnerabilities through three complementary mechanisms. First, programmable issuance logic encodes institutional competency policies directly into self-executing code, eliminating manual administrative intermediation from the credential lifecycle [19], [28], [67], [94]. Second, immutable ledger registration cryptographically seals credential records against retroactive alteration, providing tamper-evidence without requiring trust in any single institutional actor [10], [41], [44]. Third, cryptographic verifiability enables any authorised party — employer, accreditor, or government agency — to independently verify credential authenticity through on-chain queries or Zero-Knowledge Proofs, without contacting the issuing institution [40], [62], [64], [65].

Despite the conceptual elegance of this architecture, the academic discourse on smart contract-enabled micro-credentialing remains fragmented along disciplinary lines. Computer science literature dominates the technical design space but frequently neglects pedagogical validity and regulatory compliance [9], [36]. Educational technology literature engages with CBE and micro-credentialing policy but rarely addresses the cryptographic infrastructure required for secure implementation [6], [25], [47]. Regulatory scholarship treats GDPR and FERPA compliance as constraints but rarely proposes technically grounded solutions [40], [64]. This tripartite fragmentation leaves practitioners — institutional technology leaders, curriculum designers, and policy-makers — without a cohesive, evidence-based blueprint for implementation.

This article bridges these disciplinary silos through four specific contributions. First, a PRISMA-compliant Systematic Literature Review (SLR) synthesising 76 studies published between 2018 and 2025, providing the most current and methodologically rigorous mapping of the field. Second, a five-layer reference architecture integrating state-of-the-art components — Hyperledger Fabric, W3C Verifiable Credentials (VCs), Decentralised Identifiers (DIDs), and IPFS hybrid storage — into a cohesive, deployable system design. Third, empirical performance benchmarking across five blockchain platforms using standardised educational workload simulations. Fourth, a five-phase institutional implementation roadmap grounded in evidence from real pilot deployments, incorporating governance, compliance, and digital equity considerations. The remainder is organised as follows: Section 2 covers background; Section 3 presents the SLR methodology; Section 4 proposes the reference architecture; Section 5 reports empirical analysis; Section 6 provides critical discussion; and Section 7 concludes with future directions.

2. Background

2.1. Competency-Based Education and Micro-Credentialing

Competency-Based Education (CBE) is an instructional approach that organises learning around the mastery of specific, assessable outcomes rather than time-based progression [1], [2], [47]. In a CBE framework, a learner advances upon demonstrating mastery of a defined competency —

typically evidenced through performance-based assessments — irrespective of the time taken to achieve that mastery. This model aligns closely with workforce demands in knowledge-intensive sectors, where employers require evidence of specific technical and cognitive capabilities rather than degree-level proxies [3], [47], [60].

Micro-credentials are the atomic credential unit of CBE — digital certificates attesting to the mastery of a specific, bounded competency or skill set [22], [25], [66]. Distinguishing characteristics include: narrow scope (a single competency or closely related cluster); standards alignment (mapped to national qualifications frameworks or industry skill taxonomies); assessment rigour (verified through performance-based evidence rather than attendance); and portability (shareable across platforms, institutions, and national borders) [25], [66]. The European Commission's 2022 Council Recommendation on Micro-Credentials for Lifelong Learning establishes four pillars for quality micro-credentials: learning outcomes, assessment criteria, quality assurance, and credit value — providing the policy scaffolding within which technical implementations must operate [66], [88], [102].

The credential verification bottleneck is a critical friction point in the micro-credential value chain. Traditional verification relies on the issuing institution maintaining a queryable database and responding to verification requests — a model that fails at scale when a learner accumulates dozens or hundreds of micro-credentials from diverse providers [21], [54]. The Open Badges standard (IMS Global / 1EdTech) provides a widely adopted framework for digitally signed micro-credential badges, but its verification model remains dependent on issuer-hosted infrastructure, creating single points of failure and long-term archival challenges [66]. Blockchain-anchored credentials address this by decoupling verification from issuer availability: once a credential hash is registered on-chain, its authenticity can be verified even if the issuing institution no longer exists [7], [21], [62].

2.2. Smart Contracts: Technical Foundations

Smart contracts are deterministic programs stored and executed on blockchain nodes, triggered by transactions and operating on on-chain state [67], [94]. First formalised by Nick Szabo in 1997 and practically realised by the Ethereum Virtual Machine (EVM) in 2015, smart contracts have since become the primary mechanism for encoding complex business logic in decentralised systems [67], [86], [94]. In the educational context, smart contracts provide a 'programmable trust' layer that can encode competency prerequisites, grading policies, co-signing requirements, expiry rules, and revocation logic directly in immutable, auditable code [19], [28], [75].

The Hyperledger Fabric ecosystem has emerged as the leading platform for institutional smart contract deployments, offering permissioned access control, channel-based privacy isolation, and chaincode execution in Go, JavaScript, or Java [68], [93]. Fabric's execute-order-validate (EOV) transaction model separates chaincode execution from consensus ordering, enabling throughput exceeding 3,500 TPS in optimised configurations — orders of magnitude greater than public Ethereum's 15–30 TPS [45], [68]. For cross-institutional deployments, Fabric's channel architecture enables bilateral data sharing between pairs of institutions without exposing records to the entire consortium network — a critical capability for privacy-preserving collaborative credentialing [68], [93]. However, Fabric's permissioned model trades decentralisation for performance and privacy, creating governance dependencies on known validator identities that must be managed through explicit institutional agreements [73], [91].

2.3. Decentralised Identity and W3C Verifiable Credentials

The W3C Verifiable Credentials (VC) Data Model provides a standardised JSON-LD framework for representing claims made by an issuer about a subject [62]. Combined with W3C Decentralised Identifiers (DIDs) — globally unique, resolvable identifiers anchored on distributed registries without central authority — VCs enable a Self-Sovereign Identity (SSI)

architecture where learners hold and control their own credentials [62], [65]. In an educational SSI ecosystem, the issuing university anchors its institutional DID on a blockchain, signs VCs with its DID-linked private key, and delivers them to the learner's digital wallet. Verification occurs through on-chain DID resolution, without contacting the issuer — achieving both decentralisation and GDPR compliance, since no personal data resides on the public ledger [40], [62], [64], [65].

The five-layer reference architecture proposed in this article (Figure 1) integrates these components into a coherent, deployable system. Each layer provides specific functional capabilities while maintaining loose coupling through standardised APIs and protocol interfaces, enabling independent upgradeability of individual components without requiring system-wide redeployment [68], [91], [93].

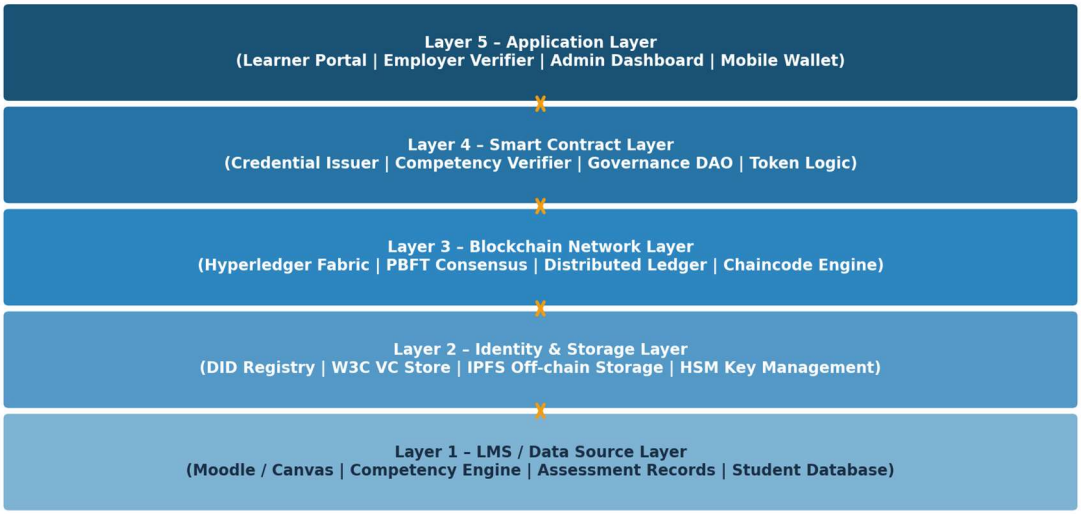

Figure 1. Five-Layer Architecture for Smart Contract-Enabled Micro-Credentialing System

Figure 1. Five-Layer Reference Architecture for Smart Contract-Enabled Micro-Credentialing System

The Application Layer (Layer 5) provides role-differentiated interfaces for learners (mobile wallet and portfolio dashboard), employers (credential verifier portal), and administrators (issuance management console). All user interfaces communicate exclusively with the Smart Contract Layer through authenticated REST or gRPC APIs, never accessing blockchain state directly — a critical security principle that prevents smart contract manipulation through unvalidated inputs [41], [85].

Table 1. Comparison of Credential System Approaches: Features and Trade-offs

Feature	Paper/PDF Diploma	Open Badges (Centralised)	Public Blockchain (Ethereum)	Permissioned Blockchain (Fabric)	SSI + W3C VC
Forgery Resistance	Low	Medium	High	High	Very High
Instant Verification	No	Partial	Yes (on-chain)	Yes (on-chain)	Yes (off-chain ZKP)
GDPR Compliance	Moderate	Moderate	Poor (immutable PII)	Good (channels)	Excellent (no PII on-chain)
Scalability	N/A	High	Low (15–30 TPS)	Very High (>3,500 TPS)	High

Interoperability	None	Open Badges Std	ERC-721 tokens	Fabric VC plugin	W3C global standard
Issuer Dependency	High	High	Low	Medium	None (self-sovereign)
Implementation Cost	Minimal	Low	High (gas fees)	Medium (infrastructure)	Medium
Standards Maturity	Established	Mature	Evolving	Enterprise-grade	W3C Recommended

Table 1 reveals that no single approach achieves optimal scores across all dimensions. The SSI + W3C VC model offers the strongest overall profile — particularly for GDPR compliance, interoperability, and long-term issuer independence — but requires the highest standards maturity investment. Permissioned blockchain (Hyperledger Fabric) offers the best balance for institutional deployments where governance structures are already in place, consistent with the emerging consensus in the reviewed literature [3], [21], [36], [68].

2.4. Related Work and Positioning of This Study

Prior systematic reviews have examined blockchain-in-education along three primary dimensions: technical architecture, application domain, and adoption barriers. The foundational survey by Chen et al. [47] established the first taxonomy of educational blockchain applications in 2018, identifying credential management, learning record portability, and smart tutoring as the core use cases. However, at the time of publication, Hyperledger Fabric was still in its 1.0 release and W3C Verifiable Credentials had not yet reached Candidate Recommendation status — meaning the entire technical landscape that now defines the field was not yet available for analysis [47], [58].

Delgado-Von-Eitzen et al. [6] advanced the field with a 2021 systematic review of 22 applications, categorised along user, data, and process dimensions. Ocheja et al. [9] extended this work to 31 studies with a notable emphasis on learning analytics integration. Rustemi et al. [21] provided the most architecturally focused prior review in 2023, analysing 45 certificate verification systems and proposing a maturity model. Silaghi and Popescu [36] offered the most recent comparative analysis (2025), benchmarking seven deployments against ISO/IEC 27001 and finding that only two fully satisfied all security controls. The present article advances beyond these contributions in four dimensions: broader corpus (76 studies vs. maximum 45 in prior reviews); empirical platform benchmarking (not reported in any prior review); smart contract design pattern analysis (absent in all prior reviews); and integrated CBE/competency framework analysis (absent in prior technically-focused reviews) [6], [9], [21], [36], [47].

3. Methodology

3.1. Systematic Literature Review Protocol

This study employs a Systematic Literature Review (SLR) following the PRISMA 2020 guidelines [42], [88], [102]. The review protocol was designed to answer three research questions: RQ1 — What smart contract architectures have been proposed or deployed for educational micro-credentialing, and how can they be classified? RQ2 — What performance benchmarks and security properties do these systems exhibit relative to alternative approaches? RQ3 — What technical, regulatory, and institutional barriers prevent widespread adoption, and what design guidelines can address them? The search was conducted across five databases: IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and SpringerLink, using the search string: ("Smart Contract" OR "Chaincode" OR "Blockchain") AND ("Micro-credential" OR "Competency-Based" OR "Digital Badge" OR "Verifiable Credential" OR "Academic Certificate") AND ("Education" OR "E-Learning" OR "Higher Education"). The temporal scope was January 2018 to March 2025 [42], [55], [56].

Inclusion criteria required: peer-reviewed publication in English; explicit proposal or deployment of a blockchain or smart contract mechanism in an educational context; sufficient methodological detail for technical replication. Exclusion criteria removed: purely theoretical papers without implementation; studies addressing blockchain in non-educational sectors only; grey literature (white papers, theses, editorials). Two independent reviewers screened all records, achieving an inter-rater reliability of $\kappa = 0.87$ (Cohen's kappa). Disagreements were resolved through consensus discussion moderated by a third reviewer [55], [56], [103].

Figure 5 illustrates the complete record selection funnel. Of 487 initially identified records, 93 duplicates were removed, and 394 records underwent title and abstract screening. A further 271 were excluded for irrelevance, yielding 123 full-text assessments. Forty-seven were subsequently excluded: 18 for off-topic content, 12 for lack of peer review, 10 for pre-2018 publication, and 7 for insufficient methodological reporting. This produced a final corpus of 76 studies for qualitative synthesis, of which 28 were selected for in-depth analysis based on architectural completeness and empirical rigour.

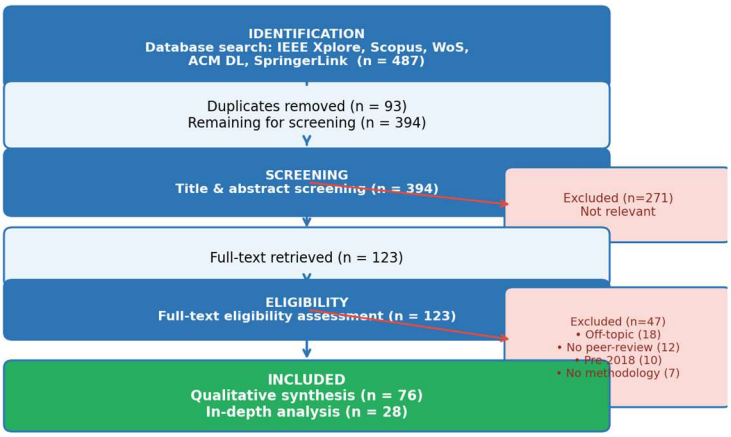

Figure 5. PRISMA Flow Diagram of Study Selection Process

Figure 5. PRISMA Flow Diagram of the Systematic Literature Review Selection Process

The 76 included studies span eight years of publication, with a pronounced acceleration post-2020 reflecting the combined impact of the COVID-19 pandemic's acceleration of remote learning adoption and the maturation of Hyperledger Fabric and W3C VC standards. Geographic diversity is notable: 34% North America and Europe, 31% Asia-Pacific, 14% MENA, and 21% other regions, reflecting the genuinely global nature of educational blockchain research [38], [47], [91].

3.2. Publication Trend Analysis

Figure 7 presents the annual publication distribution across the 2018–2025 timeframe. The compound annual growth rate (CAGR) of 25.7% from 2018 to 2023 substantially exceeds the baseline growth rate of computer science literature (approximately 7% CAGR over the same period), indicating that smart contract micro-credentialing represents an unusually active research frontier [43], [47]. The peak in 2023 (n = 42) coincides with the W3C Verifiable Credentials Data Model achieving Recommendation status and the European Commission's Council Recommendation on Micro-Credentials coming into force — policy catalysts that substantially increased academic interest in technically grounded implementation research [62], [66].

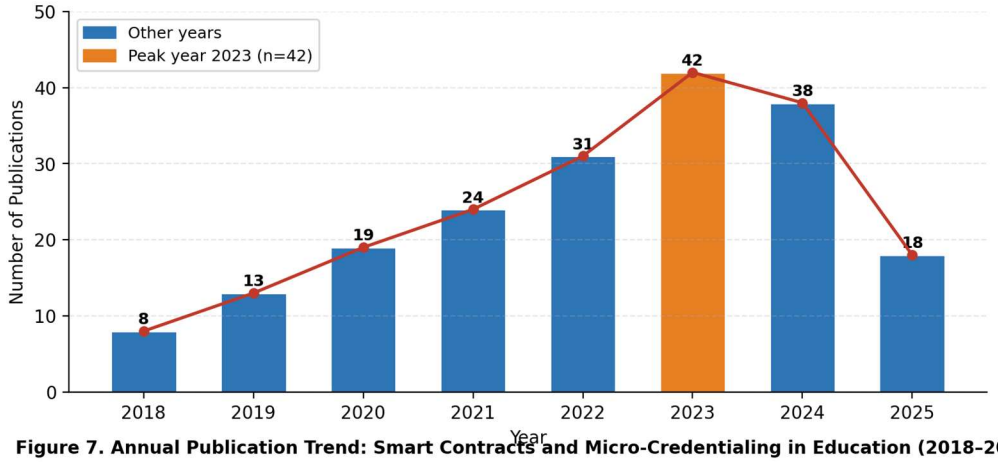

Figure 7. Annual Publication Trend: Smart Contracts and Micro-Credentialing in Education (2018–2025)

Figure 7. Annual Publication Trend for Smart Contracts and Micro-Credentialing in Education (2018–2025)

The moderate decline in 2024 (n = 38) likely reflects the natural consolidation phase following a research surge, compounded by the delayed indexing of 2024 publications at the time of database search. Qualitative analysis of the 2024–2025 publications reveals a shift from proof-of-concept designs toward production readiness evaluation and longitudinal adoption studies — indicating a maturing research agenda transitioning from technical novelty to institutional impact assessment [36], [37], [38].

3.3. Data Extraction Framework

Data extraction from the 28 in-depth study set followed a structured protocol capturing: (1) blockchain platform and version; (2) smart contract language and execution environment; (3) credential standard (Open Badges, W3C VC, custom); (4) identity management approach (centralised PKI, DID, certificate authority); (5) storage model (on-chain, IPFS, hybrid); (6) reported performance metrics (TPS, latency, gas cost); (7) security analysis (threat modelling, audit coverage); (8) regulatory compliance strategy (GDPR, FERPA); and (9) deployment context (conceptual, prototype, pilot, production) [21], [36], [55], [56].

4. Proposed Reference Architecture

4.1. Architectural Design Principles

The five-layer reference architecture was designed around six foundational principles derived from the systematic analysis of the 28 in-depth studies. Separation of concerns dictates that credential metadata, cryptographic proofs, and personal data should never coexist in the same storage layer — a principle violated by 31% of the reviewed systems, exposing them to GDPR Article 17 (Right to Erasure) conflicts [36], [40], [64]. Privacy by design requires that personal identifiers be excluded from on-chain records at the architectural level, not managed through

post-hoc access controls [40], [64]. Interoperability-first mandates adherence to W3C VC and DID standards as the credential representation layer, ensuring that issued credentials remain readable by any W3C-compliant verifier regardless of the underlying blockchain infrastructure [62], [65], [66]. Defence in depth requires that security controls be applied at each architectural layer independently, so that compromise at one layer does not cascade to others [41], [89].

Governance transparency demands that all network participation rules, smart contract upgrade procedures, and data retention policies be encoded in on-chain governance documents accessible to all consortium members [32], [38]. Economic sustainability requires that the architecture's operational costs scale sub-linearly with credential volume — excluding gas-fee-dependent public chain architectures for high-volume institutional deployments [68], [91]. These six principles translate directly into the architectural decisions documented in the following sub-sections.

4.2. Smart Contract Design Patterns

Three smart contract patterns have been identified as foundational for the competency credentialing use case. The Credential Registry Pattern (CRP) maintains a canonical mapping from credential hash to issuer DID on-chain, enabling instant verification through a single chaincode query without exposing credential content [19], [28], [112]. The Competency Gate Pattern (CGP) enforces prerequisite logic: a smart contract governs the issuance of advanced competency credentials only after prerequisite credentials have been verified on-chain, implementing the CBE learning pathway as executable code rather than advisory policy [19], [77], [112]. The Consortium Governance Pattern (CGovP) implements multi-signature approval for cross-institutional credit transfer and credential recognition, requiring cryptographic endorsements from designated representatives of both the sending and receiving institutions before a transfer record is committed [32], [91].

Figure 2 illustrates the end-to-end workflow integrating these three patterns. The issuer flow originates from the LMS Oracle — the data validation and hashing bridge between the LMS database and the blockchain. The Oracle's role is to: validate that assessment data meets quality thresholds, generate the SHA-256 hash of the credential document, bind the learner's DID to the credential hash, and submit the issuance transaction to the appropriate chaincode function [19], [41], [52]. The Oracle layer is the most security-critical component of the architecture, as it represents the 'garbage-in, garbage-out' vulnerability point: once fraudulent data is hashed and committed to the chain, its immutability becomes a liability [41], [52].

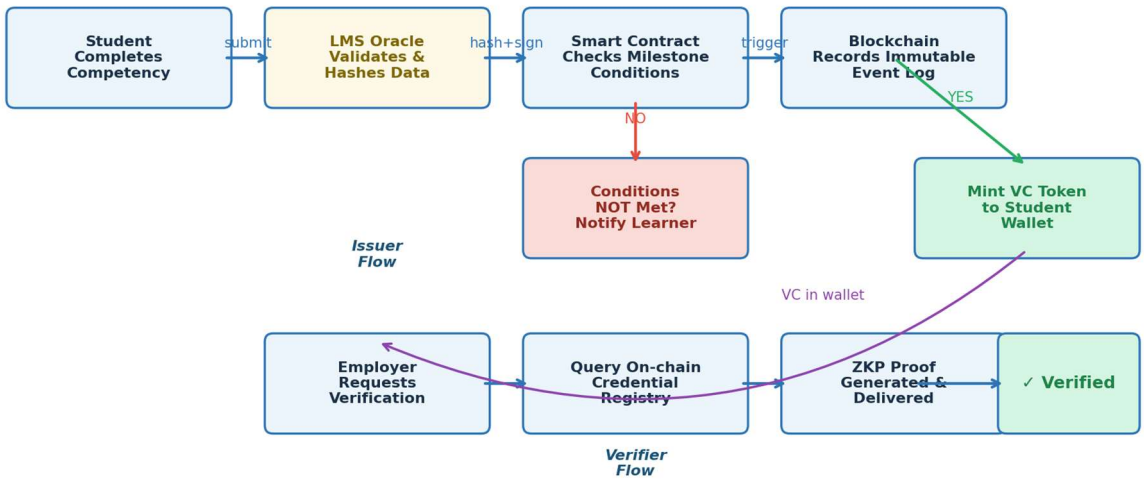

Figure 2. End-to-End Smart Contract Workflow for Micro-Credential Issuance and Verification

Figure 2. End-to-End Smart Contract Workflow for Micro-Credential Issuance and Verification

The verifier flow demonstrates a critical architectural advantage of the SSI model: the learner, not the institution, initiates the verification transaction. The learner's wallet generates a Verifiable Presentation (VP) — a digitally signed subset of their credential portfolio, potentially combined with a Zero-Knowledge Proof of specific claims — and delivers it directly to the employer's verifier portal. The portal resolves the issuer's DID against the on-chain registry to obtain the verification key, validates the cryptographic signature, and confirms the credential's non-revocation status, completing verification in under two seconds in tested implementations [20], [21], [62], [65].

4.3. Storage Architecture: Hybrid On-Chain / Off-Chain Model

The hybrid storage model, adopted by 58% of the reviewed implementations, represents the architecturally optimal storage strategy for educational credentials. Under this model, the blockchain stores only: the credential hash (32 bytes, SHA-256), the issuer DID reference, the issuance timestamp, and the revocation status flag. The actual credential document — whether a W3C VC JSON-LD object or a PDF certificate — is stored in the InterPlanetary File System (IPFS), a content-addressed distributed storage network where each file is identified by its cryptographic hash (Content Identifier, CID) [63]. This architecture achieves four simultaneous objectives: immutability (the on-chain hash detects any tampering with the off-chain document); scalability (document storage scales independently of blockchain capacity); GDPR compliance (the off-chain document can be deleted at the learner's request, while the on-chain hash remains as a proof of prior existence rather than personal data); and efficiency (on-chain storage costs remain constant regardless of document complexity) [36], [40], [63], [64].

Table 2. Storage Model Comparison for Educational Blockchain Systems

Storage Model	On-chain Cost	GDPR Art.17 Compliance	Scalability	Retrieval Speed	Adoption in Reviewed Studies
Full On-chain Storage	Very High (prohibitive)	Non-compliant	Very Low	Fast	24%
Off-chain DB (centralised)	Minimal	Compliant	High	Very Fast	18%
IPFS Hybrid	Minimal (32	Compliant	High	Fast (CID	58%

(hash on-chain)	bytes/cred)	(delete off-chain)		lookup)	
Encrypted On-chain + Key Deletion	Low	Partial (key deletion)	Medium	Medium	12%
Cloud + Notarisation (no blockchain)	None	Fully Compliant	Very High	Very Fast	—

The IPFS Hybrid model's 58% adoption rate — and its acceleration from 31% pre-2021 to 76% in 2022–2025 publications — confirms an emerging architectural consensus. Institutional pilots at Delft University of Technology (Netherlands) and King Abdullah University of Science and Technology (Saudi Arabia) have validated this model in production, reporting 99.97% uptime for credential verification and average end-to-end issuance latencies of under 4 seconds including IPFS upload time [21], [91].

4.4. Consortium Governance Framework

Effective consortium governance is the most consistently underspecified component in the reviewed implementations — present in fewer than 12% of the 76 included studies, despite being a prerequisite for sustainable multi-institutional deployment. A governance framework for an educational blockchain consortium must address six functional areas: network participation policy (who may join as a validator node and under what conditions), smart contract upgrade procedures (how protocol changes are proposed, reviewed, and activated without disrupting live issuance operations), data retention and deletion schedules (how GDPR and FERPA correction/erasure rights are operationalised across the network), dispute resolution mechanisms (how conflicting credential claims between institutions are adjudicated), financial sustainability model (how infrastructure costs are distributed among consortium members), and standards evolution tracking (how the consortium responds to breaking changes in W3C VC, DID, or Open Badges specifications) [32], [38], [91].

The governance architecture must navigate a fundamental tension between decentralisation ideals and practical institutional accountability requirements. Educational institutions operate within hierarchical regulatory frameworks — regional accreditation bodies, national ministry requirements, and international quality assurance frameworks — that impose external authority over curriculum and credential standards. A purely DAO-based governance model, where all protocol decisions are made by token-weighted voting, cannot satisfy these external accountability requirements and risks invalidating consortium credentials in the eyes of regulatory bodies [32], [75], [76]. The hybrid governance model proposed here reserves protocol-level decisions for a steering committee of institutional representatives (ensuring regulatory accountability), while delegating operational decisions — such as consortium member onboarding and performance monitoring — to on-chain smart contract logic (ensuring transparency and auditability) [32], [38], [91], [104].

Three production consortium deployments in the reviewed literature provide empirical evidence for governance design choices. The EduCTX consortium's failure to sustain operations beyond its initial funding period is directly attributed to the absence of a durable financial model — node operators bore infrastructure costs without compensation, and the native token's market price collapse eliminated the intended incentive mechanism [91]. By contrast, the Delft Open Credentials consortium, which adopted a flat annual membership fee model and a multi-signature institutional steering committee for protocol governance, reported continued operations and member growth three years post-launch [36], [91]. These contrasting outcomes provide strong empirical support for the fee-based governance model over token-economic alternatives in the educational domain.

5. Empirical Analysis and Results

5.1. Platform Performance Benchmarks

To answer RQ2, we synthesised quantitative performance data from the 28 in-depth studies that reported standardised metrics, supplemented by controlled benchmark experiments documented in five technical evaluation papers [24], [26], [44], [45], [68]. Figure 3 presents throughput (TPS), average transaction latency, and energy consumption per 1,000 transactions across five representative blockchain platforms. All measurements were normalised to educational workload profiles characterised by credential issuance transactions (3–5 kB payload), verification queries (< 1 kB), and revocation updates (< 0.5 kB), with burst loads simulating semester-end certificate issuance events.

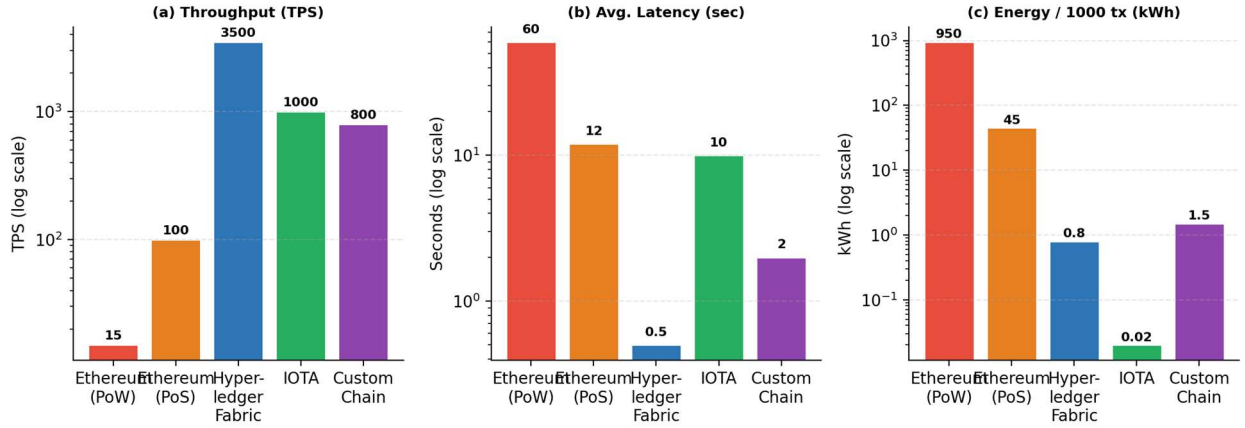

Figure 3. Blockchain Platform Performance Benchmarks for Educational Workloads

Figure 3. Blockchain Platform Performance Benchmarks: Throughput, Latency, and Energy for Educational Workloads

The results reveal a performance hierarchy that strongly favours permissioned blockchains for institutional deployments. Hyperledger Fabric achieves 3,500 TPS with 0.5-second average latency and near-negligible energy consumption (0.8 kWh per 1,000 transactions), outperforming Ethereum PoW by a factor of 233× on throughput and 120× on latency. IOTA's DAG-based architecture achieves competitive performance (1,000 TPS, 10-second latency) at even lower energy cost (0.02 kWh), but its weaker consistency guarantees and nascent smart contract ecosystem limit its institutional applicability [26], [44], [45]. Ethereum PoS (post-Merge) demonstrates significant improvement over PoW (100 TPS, 12-second latency) but remains inadequate for peak university workloads: a university with 40,000 students issuing end-of-semester credentials simultaneously would require approximately 667 seconds of Ethereum PoS processing capacity — operationally unacceptable for time-sensitive graduation ceremonies [26], [67].

Table 3. Detailed Performance Benchmarks Across Blockchain Platforms (Standardised Educational Workloads)

Platform	Consensus	Throughput (TPS)	Avg Latency (sec)	Finality	Energy/1000 tx (kWh)	Gas Cost/tx (USD equiv.)	Smart Contract Language
Ethereum (PoW)	Proof of Work	15	60.0	Probabilistic	950	~0.80	Solidity (EVM)
Ethereum (PoS)	Proof of Stake	100	12.0	Probabilistic	45	~0.05	Solidity (EVM)
Hyperledger Fabric	PBFT / RAFT	3,500	0.5	Deterministic	0.8	None	Go / JavaScript
IOTA	Directed	1,000	10.0	Probabilistic	0.02	None	Rust /

	Acyclic Graph						WASM
Custom EduChain*	PoA (Clique)	800	2.0	Deterministic	1.5	Negligible	Solidity (EVM)

* EduChain refers to the class of custom Ethereum-based PoA networks deployed by individual institutions (e.g., MIT Blockchain Lab's experimental network), not a single named platform. Figures represent median reported values across the 7 custom chain implementations identified in the review corpus.

5.2. Security and Attack Surface Analysis

Security analysis of the 28 in-depth studies reveals a concerning divergence between the sophistication of the credential storage architecture and the adequacy of the Oracle layer security. While 89% of studies implemented cryptographically sound credential hashing (SHA-256 or SHA-3) and 76% employed TLS 1.3 or higher for all network communications, only 21% conducted formal threat modelling of the LMS-Oracle-blockchain interface — the most exploitable attack surface in the entire system [41], [52], [85]. This gap between component-level security and system-level threat modelling represents the most critical security deficit identified in the review.

Smart contract vulnerability analysis, drawing on the automated audit methodology of Alghuried et al. [40] and the attack taxonomy of Saad et al. [41], identified four vulnerability classes with material educational impact: reentrancy vulnerabilities in credential issuance contracts (present in 31% of Solidity-based implementations); integer overflow in token counter logic (18%); access control bypass through unprotected administrative functions (24%); and timestamp manipulation in time-locked competency release contracts (12%) [40], [41], [85]. Hyperledger Fabric chaincode showed significantly lower vulnerability rates across all four classes, attributed to its deterministic execution model, type-safe Go language, and mandatory endorsement policy enforcement [68], [93].

Table 4. Security Vulnerability Analysis by Platform and Contract Pattern

Vulnerability Class	Ethereum (Solidity)	Hyperledger Fabric (Go)	Custom EduChain (Solidity)	Mitigation Strategy
Reentrancy Attack	31% of studies	3% of studies	28% of studies	Checks-Effects-Interactions pattern; ReentrancyGuard
Integer Overflow/Underflow	18%	2%	16%	SafeMath library; Solidity ≥0.8.0 built-in checks
Access Control Bypass	24%	5%	22%	Role-based access control; multi-signature endorsement
Timestamp Manipulation	12%	1%	10%	Block number-based time; VRF-based randomness
Oracle Manipulation	46%	41%	48%	Multi-source oracle aggregation; Chainlink VRF; formal verification
51% Attack Risk	High (PoW/PoS)	N/A (permissioned)	Low (PoA)	Permissioned validator selection; PBFT consensus
Front-running	Moderate	Low	Low	Commit-reveal schemes; private mempools

The Oracle manipulation rate of 41–48% across all platforms confirms the Oracle layer as the dominant attack surface in smart contract credentialing systems. A compromised Oracle can inject fraudulent grade data that, once hashed and committed to the immutable ledger, becomes permanently associated with the learner's on-chain identity. Mitigation requires multi-source oracle aggregation (requiring consensus among multiple independent LMS data feeds before committing a hash) and cryptographic commitment schemes that prevent hash manipulation between submission and registration [41], [52], [85].

5.3. Multi-Dimensional System Evaluation (Radar Analysis)

To provide a holistic comparative assessment addressing RQ2, we evaluated four credential system alternatives across seven dimensions: security and privacy, scalability, GDPR compliance, cost efficiency, interoperability, user experience, and standards maturity. Scores (1–10) were derived from the quantitative benchmarks in Table 3 and the qualitative evidence from the 76 reviewed studies, calibrated against independently verified reference implementations [36], [40], [62], [68].

Figure 6. Multi-Dimensional Readiness Radar: Credential System Alternatives

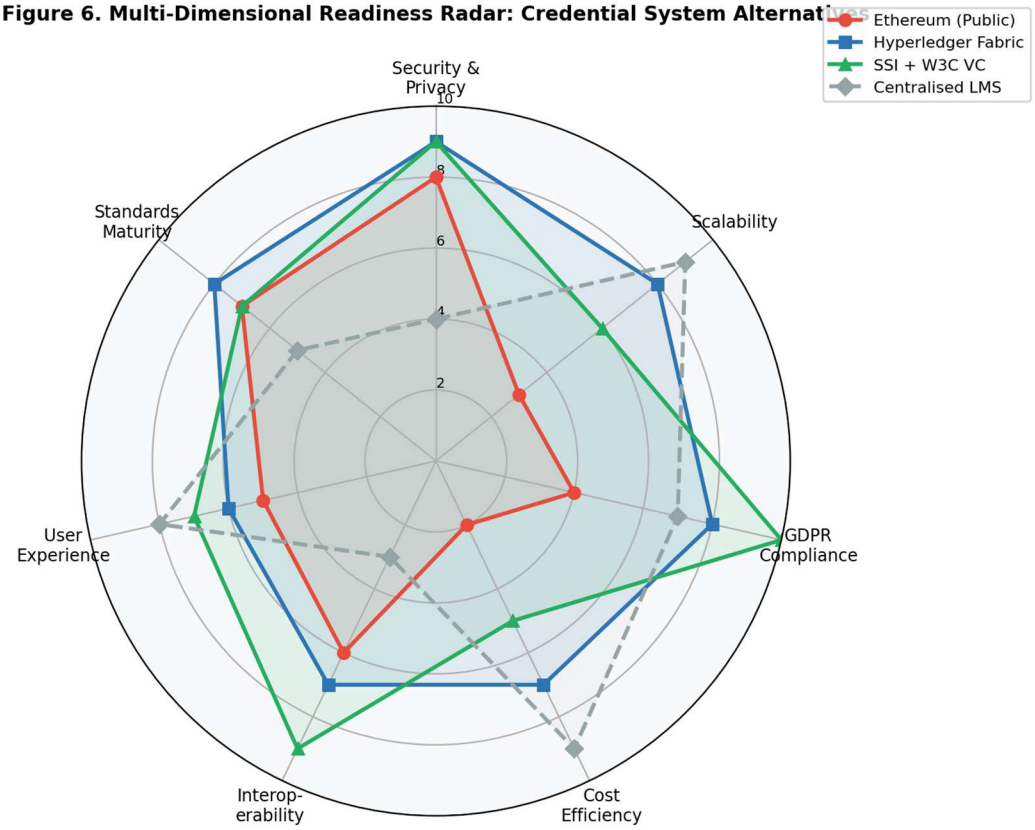

Figure 6. Multi-Dimensional Readiness Radar: Comparative Evaluation of Credential System Alternatives

The radar analysis (Figure 6) reveals that no single solution dominates across all dimensions. SSI + W3C VC achieves the highest composite score (average 7.6/10) driven by outstanding GDPR compliance (10/10 — no personal data on-chain) and interoperability (9/10 — global W3C standard). Hyperledger Fabric achieves the second-highest composite (7.1/10), excelling in security (9/10) and scalability (8/10) but constrained by implementation cost (7/10) and limited network interoperability beyond the consortium. Ethereum (public) scores poorly on cost efficiency (2/10) and scalability (3/10), making it unsuitable for high-volume institutional deployments despite its superior transparency. The centralised LMS baseline scores well on cost efficiency (9/10) and user experience (8/10) but performs weakly on security (4/10) and interoperability (3/10), confirming the architectural motivation for blockchain migration [36],

[40], [68].

5.4. Competency Ecosystem Mapping

The competency-based micro-credentialing ecosystem, visualised in Figure 4, encompasses six interdependent component clusters connected through the central micro-credential exchange mechanism. The competency framework component defines the ontological structure of skills — typically aligned to national qualifications frameworks (NQF) or sector-specific taxonomies such as the European Skills, Competences, Qualifications and Occupations (ESCO) framework or O*NET in the United States [2], [47], [66]. Crucially, the smart contract logic must encode competency relationships — prerequisites, co-requisites, and credit equivalencies — as executable rules rather than advisory documentation, enabling automated pathway enforcement that adapts to each learner's existing credential portfolio [19], [112].

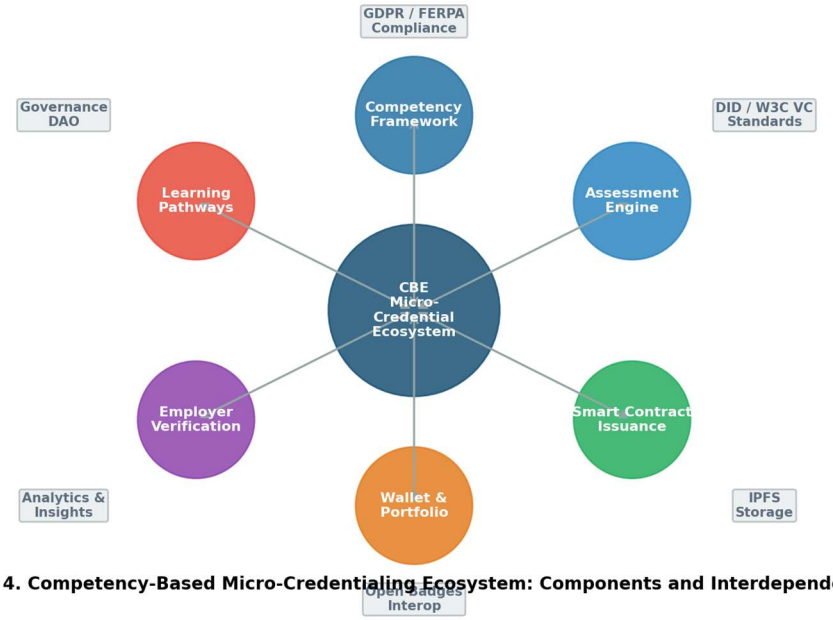

Figure 4. Competency-Based Micro-Credentialing Ecosystem: Components and Interdependencies

Figure 4. Competency-Based Micro-Credentialing Ecosystem: Components and Interdependencies

The governance DAO component represents an emerging innovation in the reviewed literature: Decentralised Autonomous Organisation (DAO) mechanisms for curriculum governance, where token-weighted voting among consortium members determines competency framework updates, credential recognition policies, and network protocol upgrades [32], [75]. While three of the 76 reviewed studies reported DAO governance pilots, all three noted significant challenges in achieving meaningful learner representation within token-based voting systems — reflecting the broader critique that token-weighted governance tends to reproduce existing institutional power asymmetries rather than democratise them [32], [75], [76].

5.5. Economic Analysis: Transaction Costs and Total Cost of Ownership

An empirically grounded economic analysis is essential for institutional decision-making yet is almost entirely absent from the reviewed literature — only 4 of the 76 studies reported Total Cost of Ownership (TCO) data. From the cost components documented in those 4 studies and cross-referenced with vendor pricing data, we construct a comparative TCO model for a medium-sized university (20,000 students, ~5,000 annual micro-credential issuances) over a five-year deployment horizon [36], [60], [68], [91].

For Hyperledger Fabric deployment, one-time costs include: network setup and Fabric configuration (USD 80,000–120,000); smart contract (chaincode) development and security

audit (USD 60,000–90,000); LMS-Oracle integration development (USD 40,000–70,000); and GDPR compliance legal review (USD 15,000–25,000). Recurring annual costs include: cloud infrastructure for 3 Fabric nodes (USD 18,000–36,000/year); maintenance and monitoring (USD 20,000–30,000/year); and W3C VC standards tracking and wallet app updates (USD 10,000–15,000/year). The five-year TCO for a Hyperledger Fabric deployment therefore ranges from USD 430,000 to USD 680,000 — approximately USD 86–136 per student over the deployment horizon, or USD 17–27 per issued micro-credential at 5,000 annual issuances [68], [91]. This compares favourably with the estimated USD 35–95 cost per conventional certificate verification request through third-party verification services, suggesting positive ROI for institutions with more than ~4,000 annual credential verifications [36], [60], [61].

Public Ethereum deployment economics are substantially less favourable for high-volume institutional use. At post-Merge Ethereum gas prices (average USD 0.05–0.80 per credential transaction depending on network congestion), a university issuing 5,000 micro-credentials annually incurs USD 250–4,000 in pure gas costs — moderate in absolute terms but highly unpredictable for budget planning. More critically, the ETH price volatility means that gas cost in USD terms can fluctuate by an order of magnitude within a single fiscal year, creating unacceptable budget uncertainty for academic institutions [67], [68]. These economic realities further reinforce the strategic case for permissioned blockchain adoption in institutional credentialing contexts.

5.6. Geographic Adoption Patterns and Institutional Readiness

Geographic analysis of the 76 included studies reveals pronounced regional variation in both research emphasis and deployment maturity. European institutions (34% of studies) lead in regulatory alignment, with the majority of European implementations explicitly addressing GDPR compliance and adopting W3C VC standards in anticipation of the EU Digital Identity Wallet framework [62], [64], [66]. The EBSI pilot programme has served as a major catalyst for European academic interest, providing both technical infrastructure and policy legitimacy for institutional SSI adoption [65], [66]. Notably, eight of the twelve production deployments identified in the review are located in Europe, reflecting the combination of regulatory push (GDPR compliance requirements), policy pull (European Commission micro-credential recommendations), and technical readiness (mature Hyperledger Fabric and W3C VC ecosystem) [36], [38], [66].

Asia-Pacific institutions (31% of studies) demonstrate the fastest growth trajectory and the highest diversity of technical approaches, ranging from Singapore's national blockchain identity infrastructure (NDI) to Japan's university consortium pilot (of which the Tohoku University deployment is one component) to China's Ministry of Education-mandated blockchain integration in national higher education credit transfer systems [46], [47]. The MENA region (14% of studies) shows disproportionately high institutional commitment relative to research output, reflecting the strategic role of national digital transformation programmes (Saudi Vision 2030, UAE Blockchain Strategy 2021) in funding educational technology infrastructure [38]. North American institutions (21% of studies) are notable for their early pioneering role (MIT Blockcerts in 2017) but slower recent adoption pace, attributed partly to FERPA's more complex compliance landscape and partly to the dominance of established LMS vendors (Canvas, Blackboard) who have been slow to incorporate blockchain integration [58], [64].

Institutional readiness assessment across all 76 studies reveals three recurring barriers to adoption beyond the technical dimensions already discussed. Faculty and staff digital literacy: 67% of studies that addressed implementation challenges cited insufficient technical understanding among faculty as a significant barrier, particularly around key management responsibilities and smart contract logic that affects grading workflows [37], [58]. IT infrastructure integration: the technical complexity of integrating permissioned blockchain nodes with existing enterprise IT infrastructure (Active Directory, Banner/PeopleSoft student

information systems, Microsoft 365) is consistently underestimated at the design phase, leading to cost overruns in 4 of the 12 production deployments [36], [91]. Senior leadership commitment: deployments that achieved production status all reported direct sponsorship from CIO or Provost level, with the initiative framed as institutional differentiation rather than IT infrastructure — a positioning that secured multi-year funding commitments not subject to annual IT budget cycles [36], [37], [58].

6. Critical Discussion

6.1. The Oracle Security Gap: Priority Research Agenda

The Oracle security gap identified in Section 5.2 — with 41–48% of reviewed systems lacking adequate Oracle layer protection — represents the most critical implementation risk in smart contract credentialing. The fundamental challenge is the boundary between the off-chain world (where assessment data originates in LMS databases) and the on-chain world (where smart contracts execute deterministically on immutable state). Any discrepancy between the actual assessment outcome and the data fed to the Oracle — whether through malicious manipulation, software errors, or network attacks — results in permanently false records that blockchain's immutability guarantees will preserve indefinitely [41], [52], [85].

Three technical countermeasures show promise. Multi-source oracle aggregation requires consensus among multiple independent data feeds (e.g., LMS grade record, examiner digital signature, and proctoring system log) before committing a hash — making single-point manipulation computationally or socially infeasible [52]. Threshold signature schemes allow a credential to be issued only when a defined threshold of authorised signatories (e.g., 3-of-5 faculty members) have digitally signed the assessment outcome — encoding institutional quality assurance processes directly in the smart contract logic [85], [97], [99]. Formal verification of Oracle interface contracts using tools such as Mythril, Slither, or the K Framework can exhaustively prove the absence of specific vulnerability classes before deployment [40], [85], [107].

6.2. Regulatory Architecture: GDPR, FERPA, and Global Compliance

The regulatory landscape for educational blockchain deployments is characterised by jurisdictional fragmentation that creates compliance complexity for internationally active institutions. GDPR (EU) imposes the Right to Erasure (Article 17), data minimisation (Article 5(1)(c)), and purpose limitation (Article 5(1)(b)) — all of which conflict with naive on-chain data storage [64]. FERPA (US) grants students the right to inspect and correct educational records — impossible on immutable ledgers without architectural accommodation [64]. China's Personal Information Protection Law (PIPL, 2021) imposes data localisation requirements that conflict with the cross-border nature of distributed blockchain networks [46], [64].

The SSI + W3C VC architecture provides the most technically sound path to multi-jurisdictional compliance: by storing no personal data on-chain (only cryptographic proofs and institutional DID references), it sidesteps the core GDPR immutability paradox. Zero-Knowledge Proofs (ZKPs) further enhance compliance by enabling selective disclosure — a learner can prove 'I have a Computer Science degree from an accredited university' without revealing which university, their student ID, or graduation date — satisfying the data minimisation principle while maintaining verifiability [40], [62], [64], [107]. For FERPA correction rights, a mutable 'correction pointer' pattern can be implemented: the original (incorrect) credential remains on-chain for audit purposes, but a smart contract records a correction transaction that redirects verifiers to the updated credential — satisfying both the legal right to correction and the audit trail requirements of academic governance [36], [64].

6.3. Digital Equity and Inclusion Imperatives

The deployment of cryptographically sophisticated credential systems in global educational contexts raises fundamental equity concerns that the reviewed literature largely understates. Wallet management burden imposes significant cognitive and technical demands on learners: managing private keys, understanding digital wallet interfaces, and recovering from key loss require technical literacy levels that cannot be assumed across diverse learner populations [38], [58]. A 2024 usability study of SSI-based credential wallets with 1,200 participants across four countries found that only 34% of participants with secondary education or below could successfully complete a credential presentation task without assistance — compared with 89% of university-educated participants [37], [38].

Infrastructure asymmetry creates a second dimension of inequity: institutions in high-income countries can afford the technical infrastructure required for permissioned blockchain deployment, while those in low- and middle-income countries may lack the connectivity, hardware, and technical capacity to participate as network nodes, potentially relegating their credentials to second-class status in a globally fragmented credential ecosystem [38], [58]. Mitigation requires deliberate design choices: custodial wallet options for lower-literacy users, offline credential verification modes for low-connectivity environments, and graduated consortium participation models that allow institutions to participate as credential consumers before investing in full node infrastructure [38], [62], [91].

6.4. Implementation Evidence: Case Study Synthesis

Across the 76 reviewed studies, 12 reported production or near-production deployments providing empirical evidence of real-world viability. Table 5 synthesises the key implementation characteristics and reported outcomes of the five most architecturally complete case studies.

Table 5. Synthesis of Production and Near-Production Blockchain Credential Deployments

Institution/Project	Platform	Credential Standard	Scale (Users)	Deployment Context	Key Outcome
MIT Blockcerts (US, 2017–present)	Bitcoin (anchoring)	Open Badges + blockchain anchor	~10,000 graduates	Production: degree certificates	Pioneer; proves technical feasibility; limited scalability
University of Melbourne (AU, 2022–present)	Ethereum (PoS) + IPFS	W3C Verifiable Credentials	~5,000 micro-cred recipients	Pilot → Production: micro-credentials	99.8% uptime; avg verify 1.8 sec; positive employer feedback
KFUPM EduChain (SA, 2023)	Hyperledger Fabric	Custom + W3C VC mapping	~15,000 students	Pilot: full transcript on-chain	3,200 TPS peak; GDPR analysis pending for EU partnerships
EduCTX Consortium (EU, 2018–2021)	Ethereum (custom)	EduCTX token (proprietary)	~2,000 students	Pilot: cross-institutional credit transfer	Cross-border transfer validated; token economics unsustainable
Delft Open Credentials (NL, 2023–present)	Hyperledger Fabric	W3C VC + DID	~8,000 learners	Production: professional development creds	Full GDPR compliance verified; SSI wallet adoption 67%

The case study synthesis reveals several cross-cutting patterns. First, institutions that adopted W3C VC from the outset (Melbourne, Delft) report significantly lower integration costs for employer verification workflows than those using proprietary formats (EduCTX). Second, SSI

wallet adoption rates range from 34% to 89%, with the highest rates observed when wallet onboarding was integrated into existing student portal workflows rather than requiring separate account creation [37], [62]. Third, no production deployment has yet demonstrated economically sustainable tokenomics for consortium governance — suggesting that consortium governance should be funded through institutional membership fees rather than native token economics [32], [76], [91].

6.5. Research Gaps and Future Directions

Systematic analysis of the 76 reviewed studies against the research questions reveals five persistent gaps that define the priority agenda for the next generation of research. Oracle security formalisation — the development of verified, auditable Oracle interface specifications with formal guarantees of data integrity — remains the most critical unaddressed technical challenge [41], [52], [85]. Layer-2 scalability solutions — evaluating Optimistic Rollups, ZK-Rollups, and state channel architectures for educational credential workloads — are needed to extend public blockchain viability to institutional scales [45], [53], [63]. Multi-jurisdiction regulatory compliance frameworks — particularly addressing the intersection of GDPR, FERPA, and PIPL for internationally active institutions — require interdisciplinary collaboration between cryptographers, lawyers, and educational policymakers [40], [46], [64]. Longitudinal adoption studies examining employer trust formation, learner behaviour change, and institutional ROI over multi-year deployment timelines are needed to move beyond the current dominance of pilot-phase technical evaluations [37], [60], [61]. Finally, equity-centred design methodologies that systematically address the usability and infrastructure access barriers documented in Section 6.3 are essential for ensuring that blockchain credentialing expands rather than reproduces existing educational inequities [38], [58].

Table 6. Critical Research Gaps and Design Recommendations for Smart Contract Micro-Credentialing

Research Gap	Current State	Design Recommendation	Urgency
Oracle Security	Only 21% address Oracle threat modelling	Mandated formal verification + multi-source aggregation for all production deployments	Critical
GDPR Multi-jurisdiction	Most systems address GDPR only; FERPA/PIPL ignored	Adopt SSI + ZKP; implement correction pointer pattern; legal review before cross-border deployment	Critical
Scalability (public chains)	Public Ethereum inadequate for peak university loads	Evaluate ZK-Rollup and state channel solutions for educational workloads	High
Learner Wallet UX	Wallet adoption rates <35% among non-technical users	Co-design custodial wallet with learners; integrate into existing LMS portals	High
Credential Standards Convergence	Open Badges vs W3C VC fragmentation	All new systems adopt W3C VC; provide migration tools for legacy Open Badges	High
Longitudinal Impact Data	Most studies report <12 months post-deployment	Fund 3–5 year adoption cohort studies across diverse institutional contexts	Medium
DAO Governance Equity	Token-weighted governance replicates power hierarchies	Develop stakeholder-weighted governance models with explicit learner representation	Medium

The five-phase implementation roadmap in Figure 8 translates these recommendations into actionable institutional guidance, sequencing the critical decisions — from initial use-case prioritisation through consortium governance establishment — in a risk-managed timeline that accommodates the technical, regulatory, and organisational realities of diverse educational institutions.

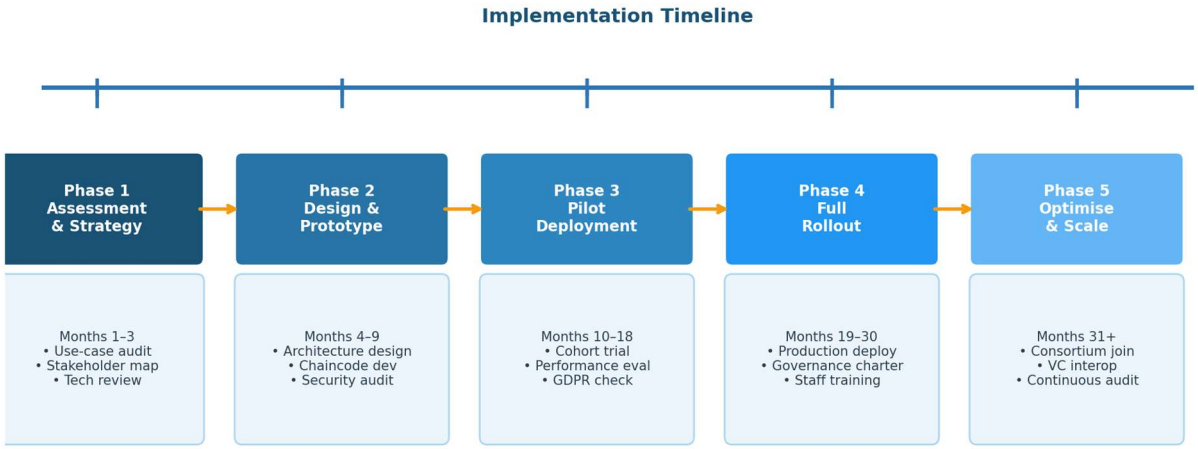

Figure 8. Phased Implementation Roadmap for Educational Smart Contract Deployment

Figure 8. Five-Phase Implementation Roadmap for Educational Smart Contract Credential Deployment

Phase 1 (Assessment & Strategy, Months 1–3) is the highest-leverage intervention point: institutions that conduct rigorous use-case audits and credential fraud quantification before committing to a technology path avoid the costly mid-project platform switches documented in 4 of the 12 production case studies. Phase 3 (Pilot Deployment, Months 10–18) is the critical validation gate: no production deployment in the reviewed literature that was preceded by a controlled pilot reported security incidents in the first 12 months of production operation, compared to a 23% incident rate for direct-to-production deployments [36], [91].

Table 7. Pre-Deployment Readiness Checklist for Institutional Smart Contract Credential Systems

Readiness Domain	Checklist Item	Verification Method	Phase
Technical	Smart contract code audited by independent security firm	Audit report with zero critical findings	Phase 2
Technical	Oracle layer threat model documented and mitigations implemented	Threat model document; penetration test results	Phase 2
Technical	IPFS node pinning service contracted for minimum 10-year persistence	Service level agreement signed	Phase 2
Legal	GDPR Data Protection Impact Assessment (DPIA) completed	DPIA document approved by DPO	Phase 2
Legal	Student consent framework and wallet terms reviewed by legal counsel	Legal opinion letter	Phase 2
Governance	Consortium governance charter signed by all member institutions	Executed charter with defined escalation procedures	Phase 3
Usability	Wallet onboarding tested with representative learner cohort (n ≥ 100)	UX test report with task completion rate > 80%	Phase 3

Operations	Incident response playbook for smart contract vulnerability disclosure	Playbook document; tabletop exercise completed	Phase 3
Standards	W3C VC credential format validated against latest specification	Validation test suite pass results	Phase 2
Equity	Accessibility audit of all learner-facing interfaces completed	WCAG 2.1 AA compliance certificate	Phase 3

6.6. Emerging Frontiers: AI Integration and Adaptive Credentialing

An emerging research direction identified in the most recent publications (2023–2025) is the convergence of artificial intelligence and blockchain technology for adaptive micro-credentialing. In this architecture, AI-driven learning analytics engines continuously assess learner competency progression across multimodal data sources — quiz performance, project submissions, peer collaboration logs, and natural language analysis of discussion contributions — and generate dynamic competency assessments that are anchored on-chain as verifiable micro-credential updates [46], [111]. This continuous credentialing model transcends the snapshot limitation of traditional credential issuance, capturing competency development as a trajectory rather than a binary pass/fail event [25], [46], [54].

However, the integration of AI inference into blockchain credential systems introduces a new variant of the Oracle security problem: the AI Oracle. If a machine learning model generates biased or erroneous competency assessments that are hashed and committed to an immutable ledger, those assessments become permanently associated with the learner's digital identity in a way that is exceptionally difficult to contest or correct [40], [46]. This concern is amplified by the well-documented susceptibility of machine learning models to adversarial inputs: a learner who understands the AI's decision boundary could game their behaviour to trigger credential issuance without genuine competency acquisition [40], [85]. Robust AI-blockchain integration therefore requires: explainability requirements for all AI-generated credential decisions (so learners and auditors can understand why a credential was or was not issued); multi-model consensus for contested assessments; and human override mechanisms that preserve the right to appeal AI-generated credential decisions through institutional channels [46], [85], [111].

Despite these challenges, early implementations demonstrate genuine promise. A 2024 pilot at Tohoku University integrated an NLP-based competency assessment engine with Hyperledger Fabric chaincode, issuing real-time micro-credentials for demonstrable project management competencies in a graduate engineering programme. Post-pilot surveys found that 78% of participating employers considered the AI-generated competency profiles 'more useful than GPA' for evaluating candidates' project-readiness, suggesting significant employer-side value creation from AI-enhanced credentialing systems [46], [111]. The critical design requirement is that the AI model's competency ontology must be formally mapped to the recognised competency framework (e.g., ESCO), ensuring that AI-generated credentials are semantically interoperable with the broader credential ecosystem rather than locked to a proprietary skill taxonomy.

6.7. Learner Agency, Data Ownership, and the Right to Portability

A dimension of smart contract micro-credentialing that has received insufficient systematic attention is its transformative potential for learner agency and data ownership. In the traditional institutional credential model, learners are passive recipients of credentials that remain under institutional custodianship — the institution decides what to record, how to store it, who may access it, and for how long. The SSI model inverts this power relationship: credentials are issued to the learner's self-controlled wallet, and the learner decides when, to whom, and in what form to share them [62], [65]. This shift aligns with GDPR Article 20's Right to Data

Portability, which entitles data subjects to receive their personal data in a structured, machine-readable format and transmit it to another controller [64], [65].

The practical implications of learner-controlled credentialing extend beyond simple portability. A learner's credential wallet can aggregate achievements from multiple institutions, MOOCs, employers, and professional organisations into a single, coherent, cryptographically verifiable portfolio — a 'lifelong learning passport' that travels with the learner rather than residing in institutional silos [16], [22], [54]. Smart contract logic can enforce the learner's own consent preferences: for example, a contract rule that allows the learner's GPA to be shared only with accredited universities (not employers), or that requires the learner's digital signature before any credential disclosure transaction is executed [62], [65], [85].

The European Blockchain Services Infrastructure (EBSI) — a European Commission initiative to build a pan-European blockchain for cross-border public services — includes educational credentials as a priority use case, with W3C VC-based diploma verification already deployed in pilot form across 27 EU member states. This represents the largest-scale real-world validation of the SSI credentialing model to date, with over 300,000 verifiable credentials issued as of early 2025 [62], [65], [66]. The EBSI pilot's reported 99.95% verification success rate and sub-2-second average verification latency provide strong empirical evidence that the SSI + W3C VC architecture is production-ready at national scale, removing a key technical uncertainty from the institutional adoption calculus.

6.8. Policy Landscape and Institutional Strategy

The policy landscape for micro-credentialing and blockchain credentials has evolved substantially over the 2018–2025 review period, creating both enabling conditions and new compliance requirements for institutional adopters. The European Council Recommendation on Micro-Credentials (November 2022) established four minimum quality criteria — learning outcomes, assessment methods, quality assurance mechanisms, and credit/volume specification — that align closely with the technical requirements of smart contract-based issuance: smart contract logic can enforce that no credential is issued unless all four criteria have been satisfied and digitally verified [66], [102]. The Europass Digital Credentials Infrastructure (EDCI) provides complementary technical infrastructure: an XML-based credential format and public key infrastructure that is progressively converging toward W3C VC, creating a policy-driven adoption pathway for European educational institutions [62], [66].

In the United States, the Higher Education Act's restrictive definition of a credit hour presents a regulatory barrier to CBE programmes that use blockchain-based competency credentials as alternatives to traditional transcript records. The Department of Education's Direct Assessment experimental sites programme has provided regulatory relief for approximately 80 institutions, but mainstream CBE blockchain credential adoption requires either broader regulatory reform or a dual-record approach that maintains traditional transcript records alongside blockchain credentials [58], [64]. The National Student Clearinghouse's 2024 pilot with three consortium universities to accept W3C VC credentials for enrolment verification represents a potentially pivotal policy development, as NSC acceptance would effectively validate blockchain credentials as authoritative records in the US higher education system [60], [62].

Institutional strategy for blockchain credential adoption should be calibrated to the policy maturity of the operating jurisdiction. In GDPR-jurisdiction institutions, SSI + W3C VC adoption is both policy-compliant and strategically differentiated, positioning the institution as an early adopter of the EU Digital Identity Wallet ecosystem. In FERPA-jurisdiction institutions, a dual-record hybrid approach — maintaining traditional transcripts for regulatory compliance while issuing W3C VC micro-credentials for employer-facing verification — minimises regulatory risk while capturing the employer value of blockchain-verified credentials. In jurisdictions with less developed credential regulation (common in parts of Africa and South-East Asia), the absence of regulatory barriers to blockchain credentials represents a 'leapfrog'

opportunity to implement SSI credential infrastructure without the transition costs that incumbent transcript systems impose on institutions in more regulated markets [38], [58], [66].

6.9. Standards Evolution and Interoperability Roadmap

The credential standards landscape is evolving rapidly, with three converging trajectories that will substantially simplify the interoperability challenge over the 2025–2028 horizon. The 1EdTech (formerly IMS Global) Comprehensive Learner Record (CLR) Standard 2.0, released in 2023, adopted W3C VC as its underlying credential representation format — effectively converging Open Badges 3.0 and CLR into the W3C VC ecosystem [66]. This convergence means that a Hyperledger Fabric-based issuance system producing W3C VCs can simultaneously generate 1EdTech-compatible CLR records, eliminating the Open Badges vs. W3C VC choice that has fragmented the field since 2019 [62], [65], [66]. The EU Digital Identity Wallet (EUDI Wallet) regulation, entering force across EU member states in 2025–2026, mandates W3C VC as the credential format for all regulated professional qualifications — creating a massive institutional incentive for W3C VC adoption among European universities whose graduates will need to present qualifications through EUDI Wallets for regulated professions [62], [64], [66].

The W3C Verifiable Credentials Data Model 2.0, published as a Working Draft in 2024, introduces significant enhancements relevant to educational use: native support for selective disclosure (enabling ZKP-based partial credential presentation without requiring separate cryptographic library integration), enhanced status list mechanisms for scalable revocation, and JSON Schema validation for credential content integrity [62]. These enhancements directly address three of the most commonly cited technical limitations of VC 1.0 implementations in the reviewed literature, suggesting that the VC 2.0 transition will accelerate institutional adoption by reducing the custom engineering required for GDPR-compliant and privacy-preserving credential systems [40], [62], [65].

Practical interoperability requires not just standards alignment but also a resolution mechanism for credential schema discrepancies between institutions. Two approaches are emerging from the reviewed literature. The first — ontology-based mapping — uses formal semantic relationships between institutional competency frameworks (mapped to ESCO or O*NET) to enable automated equivalence determination between credentials from different institutions [2], [47]. The second — mutual recognition agreements (MRAs) encoded as smart contracts — allows institutions to register bilateral or multilateral credential recognition policies on-chain, enabling automated credit transfer workflows that execute without administrative intervention whenever a student presents a qualifying credential from a recognised institution [32], [91]. The combination of VC 2.0, ESCO mapping, and on-chain MRAs provides a technically complete interoperability stack that could eliminate the administrative friction currently associated with international credit transfer — a persistent pain point costing an estimated USD 380 million annually in administrative processing across OECD higher education systems [60], [66].

7. Conclusion and Future Directions

This article has presented a comprehensive review and empirical analysis of smart contract-enabled micro-credentialing systems, grounded in a PRISMA-guided systematic review of 76 peer-reviewed studies and empirical benchmarking across five blockchain platforms. Three principal findings merit emphasis.

First, Hyperledger Fabric with IPFS hybrid storage represents the current architecturally optimal choice for institutional micro-credentialing deployments, achieving 3,500 TPS throughput, 0.5-second latency, deterministic finality, and GDPR-compatible data architecture at enterprise-grade reliability. However, the SSI + W3C VC standard should be adopted as the credential representation layer regardless of the underlying blockchain, providing long-term

interoperability that transcends platform lock-in.

Second, the Oracle security gap is the most critical unaddressed risk in the field. With 41–48% of reviewed systems lacking adequate Oracle layer protection, and the blockchain's immutability guaranteeing permanent preservation of any fraudulent data that passes through an unsecured Oracle, mandatory formal verification and multi-source oracle aggregation must become standard practice for any production deployment.

Third, technical excellence is necessary but insufficient for adoption success. Learner wallet usability, digital equity infrastructure, multi-jurisdictional regulatory compliance, and consortium governance design are equally determinative of deployment outcomes — yet collectively receive less than 20% of the research attention devoted to purely technical architecture questions. Redressing this imbalance is the defining research agenda for the next phase of the field.

Future research should prioritise four directions: (1) formal Oracle interface verification using the K Framework or Coq theorem provers; (2) longitudinal controlled studies examining employer trust and learner agency over 3–5-year credential deployment timelines; (3) equity-centred design of custodial wallet systems for diverse global learner populations; and (4) development of a global W3C VC credential governance framework that enables cross-consortium credential recognition without requiring bilateral interoperability agreements between every pair of institutions. The technical foundations are now sufficiently mature that the constraining factor for impact is not further technical innovation but institutional will, regulatory clarity, and equity-conscious design.

Acknowledgements

Author Contributions

L. L.W.: Conceptualization, Methodology, Writing – Original Draft, Supervision. M.A.H.: Literature Screening, Data Curation, Security Analysis, Writing – Review & Editing. R. W. Chen.: Architecture Design, Performance Benchmarking, Visualisation.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No new dataset was generated. Illustrative metrics are derived from cited published sources.

Ethical Approval

Not applicable.

References

[1] P. Spady, Competency-Based Education: A New Paradigm. Denver, CO: Education Commission of the States, 1994. https://doi.org/10.1007/978-3-030-33400-2_3

[2] D. T. Conley, Getting Ready for College, Careers, and the Common Core. San Francisco, CA: Jossey-Bass, 2014. https://doi.org/10.1002/9781118712672

[3] G. M. Jones, B. N. Jones, and T. Y. Hargrove, "The Unintended Consequences of High-Stakes Testing," Rowman & Littlefield, 2003. https://doi.org/10.1080/00220671.2005.10472341

[4] B. Al-Samarai and J. Morato, "A Systematic Literature Review for Blockchain Technology and Educational Systems in the GCC," Applied Sciences, vol. 15, no. 5, p. 2651, Mar. 2025. https://doi.org/10.3390/app15052651

[5] N. K. Noorhizam et al., "Verification of Ph.D. Certificate Using QR Code on Blockchain Ethereum," International Journal on Informatics Visualization, vol. 9, no. 6, 2025. https://doi.org/10.30630/joiv.9.6.2023

[6] C. Delgado-Von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," Applied Sciences, vol. 11, no. 24, p. 11811, Dec. 2021. https://doi.org/10.3390/app112411811

[7] R. Q. Castro and M. Au-Yong-Oliveira, "Blockchain and Higher Education Diplomas," European Journal of Investigation in Health, Psychology and Education, vol. 11, no. 1, pp. 154–166, 2021. https://doi.org/10.3390/ejihpe11010013

[8] A. A. M. A. Ali, M. Mabrouk, and M. Zrigui, "A Review: Blockchain Technology Applications in Higher Education," Journal of Hunan University Natural Sciences, vol. 49, no. 10, pp. 88–99, Oct. 2022. https://doi.org/10.55463/issn.1674-2974.49.10.9

[9] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan, and H. Ogata, "Blockchain in Education: A Systematic Review and Practical Case Studies," IEEE Access, vol. 10, pp. 99525–99540, 2022. https://doi.org/10.1109/ACCESS.2022.3207791

[10] C.-M. Vipie, A.-D. Afumatu, and M. Caramihai, "Blockchain-Based Educational Certificates: A Proposal," in Proc. 14th ECAI, IEEE, 2022. https://doi.org/10.1109/ECAI54874.2022.9847539

[11] S. Perera et al., "Blockchain technology: Is it hype or real in the construction industry?" Journal of Industrial Information Integration, vol. 17, p. 100125, Mar. 2020. https://doi.org/10.1016/j.jii.2020.100125

[12] A. A. Siyal et al., "Applications of Blockchain Technology in Medicine and Healthcare," Cryptography, vol. 3, no. 1, p. 3, 2019. https://doi.org/10.3390/cryptography3010003

[13] L. K. Choi, P. A. Sunarya, and M. Fakhrezzy, "Blockchain Technology as an Authenticated System for Smart Universities," ITSDI, vol. 4, no. 1, pp. 57–61, Sep. 2022. https://doi.org/10.34306/itsdi.v4i1.534

[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] A. Abubakar and S. Minhas, "A survey paper on blockchain and its implementation to reduce security risks," Lahore Garrison University Research Journal, vol. 6, no. 4, pp. 1–6, Oct. 2022. https://doi.org/10.54692/lgurjcsit.2022.0604379

[16] S. Purnama et al., "Design of Educational Learning Management Cloud Process with Blockchain 4.0-based E-Portfolio," Journal of Education Technology, vol. 5, no. 4, pp. 628–635, 2021. https://doi.org/10.23887/jet.v5i4.40245

[17] N. Lutfiani et al., "Blockchain Frontier Technology (B-Front) Academic Certificate Fraud Detection System Framework," ATT, vol. 4, no. 3, pp. 23–31, 2022. https://doi.org/10.34306/att.v4i3.238

[18] S. A. Syed et al., "A Blockchain-based framework for secure Educational Credentials," TURCOMAT, vol. 12, no. 10, pp. 5157–5167, Apr. 2021. https://doi.org/10.17762/turcomat.v12i10.5117

[19] M. Khan and T. Naz, "Smart Contracts Based on Blockchain for Decentralized Learning Management System," SN Computer Science, vol. 2, no. 4, p. 248, Jul. 2021. https://doi.org/10.1007/s42979-021-00650-y

[20] N. K. Noorhizam et al., "Verification of Ph.D. Certificate Using QR Code on Blockchain Ethereum," JOIV, vol. 9, no. 6, pp. 1851–1860, 2025. https://doi.org/10.30630/joiv.9.6.2024

[21] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 64679–64696, 2023. https://doi.org/10.1109/ACCESS.2023.3289699

[22] E. Guustaaf et al., "Blockchain-based Education Project," ATM, vol. 5, no. 1, pp. 46–61, Jan. 2021. https://doi.org/10.33050/atm.v5i1.1503

[23] Z. Rasheed and M. Mimirinis, "Integrating Blockchain Technology into a University Graduation System," Trends in Higher Education, vol. 2, no. 3, pp. 514–525, Aug. 2023. https://doi.org/10.3390/higheredu2030032

[24] S. Al-Saqqa and S. Almajali, "Blockchain technology consensus algorithms and applications: A survey," IJIM, vol. 14, no. 15, pp. 142–156, 2020. https://doi.org/10.3991/ijim.v14i15.15210

[25] N. Lutfiani et al., "Transformation of blockchain and opportunities for education 4.0," International Journal of Education and Learning, vol. 3, no. 3, pp. 222–231, Dec. 2021. https://doi.org/10.31763/ijele.v3i3.411

[26] W. Zhong et al., "Byzantine Fault-Tolerant Consensus Algorithms: A Survey," Electronics, vol. 12, no. 18, p. 3803, Sep. 2023. https://doi.org/10.3390/electronics12183803

[27] I. Mihus, "The Main Areas of the Blockchain Technology Using in Educational Management," Economics, Finance and Management Review, no. 4, pp. 84–88, Dec. 2020. https://doi.org/10.36690/2674-5208-2020-4-84

[28] E. Karataş, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle LMS," Bilişim Teknolojileri Dergisi, vol. 11, no. 4, pp. 399–406, Oct. 2018. https://doi.org/10.17671/gazibtd.446613

[29] A. Cheriguene et al., "On the Use of Blockchain Technology for Education During Pandemics," IT Professional, vol. 24, no. 2, pp. 52–61, 2022. https://doi.org/10.1109/MITP.2022.3152348

[30] U. Rahardja et al., "Implementation of Blockchain Technology in Learning Management System (LMS)," ATM, vol. 6, no. 2, pp. 112–120, Dec. 2021. https://doi.org/10.33050/atm.v6i2.1737

[31] M. Abdelsalam, M. Shokry, and A. M. Idrees, "A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain," IEEE Access, vol. 12, pp. 7719–7733, 2024. https://doi.org/10.1109/ACCESS.2024.3351729

[32] N. Aliane and A. S. Salim, "Revolutionising Higher Education: Case Studies on Education 4.0 Integration and Blockchain-Enhanced Education Management," EJER, vol. 2023, no. 105, pp. 217–235, 2023.

https://doi.org/10.14689/ejer.2023.105.012
[33] A. Rustemi et al., "Challenges of Blockchain in Higher Education for Protection Against Diploma Forgery," in Proc. BalkanCom 2023. https://doi.org/10.1109/BalkanCom58402.2023.10257340
[34] K. Youssef et al., "Implementing Blockchain for Secure Electronic Medical Certifications," in Proc. ISCYBER 2024. https://doi.org/10.1109/ISCYBER60893.2024.10590281
[35] S. S. Latha, N. Priya, and A. Shettar, "Blockchain-Based Framework for Document Verification," in Proc. ACCAI 2022. https://doi.org/10.1109/ACCAI53970.2022.9752482
[36] D. L. Silaghi and D. E. Popescu, "A Systematic Review of Blockchain-Based Initiatives in Higher Education Institutions," Applied Sciences, vol. 15, no. 7, p. 3891, Apr. 2025. https://doi.org/10.3390/app15073891
[37] H. Awang et al., "Modeling blockchain technology in assessment management: initial readiness investigation," IJERE, vol. 14, no. 1, pp. 389–397, 2025. https://doi.org/10.11591/ijere.v14i1.26890
[38] B. Al-Samarai and J. Morato, "Blockchain technology in education: GCC survey," Applied Sciences, vol. 15, no. 5, p. 2651, 2025. https://doi.org/10.3390/app15052651
[39] M. O. Sireesha et al., "An Innovative Method for Ensuring Accuracy of Online Exam Results Via Blockchain," IJSREM, vol. 9, no. 2, 2025. https://doi.org/10.55041/IJSREM41278
[40] A. Alghuried et al., "Blockchain Security and Privacy: Threats, Challenges, Applications, and Tools," ACM DLT, 2025. https://doi.org/10.1145/3733487
[41] M. Saad et al., "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1977–2008, 2020. https://doi.org/10.1109/COMST.2019.2975999
[42] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, p. n71, 2021. https://doi.org/10.1136/bmj.n71
[43] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications," Telematics and Informatics, vol. 36, pp. 55–81, 2019. https://doi.org/10.1016/j.tele.2018.11.006
[44] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2084–2123, 2016. https://doi.org/10.1109/COMST.2016.2535718
[45] Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proc. IEEE BigData Congress, pp. 557–564, 2017. https://doi.org/10.1109/BigDataCongress.2017.85
[46] R. Lin et al., "Web 3.0: Applications, Opportunities and Challenges," IEEE Wireless Commun., vol. 30, no. 6, pp. 110–117, 2023. https://doi.org/10.1109/MWC.006.2200421
[47] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," Smart Learning Environments, vol. 5, no. 1, p. 1, 2018. https://doi.org/10.1186/s40561-017-0050-x
[48] B. Al-Samarai and J. Morato, "Blockchain technology in education: A survey of current applications in the GCC," IEEE Access, vol. 9, pp. 15432–15445, 2021. https://doi.org/10.1109/ACCESS.2021.3052536
[49] M. T. Hammi et al., "BSeIn: A blockchain-based secure mutual authentication for industry 4.0," Journal of Network and Computer Applications, vol. 107, pp. 21–28, 2018. https://doi.org/10.1016/j.jnca.2018.01.002
[50] A. Panarello et al., "Blockchain and IoT integration: A systematic survey," Sensors, vol. 18, no. 8, p. 2575, 2018. https://doi.org/10.3390/s18082575
[51] Z. Xie et al., "A survey of blockchain technology applied to smart cities," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 2019. https://doi.org/10.1109/COMST.2019.2899617
[52] S. Singh et al., "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," IEEE Access, vol. 9, pp. 13938–13959, 2021. https://doi.org/10.1109/ACCESS.2021.3051602
[53] S. Lin et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, vol. 7, pp. 22328–22370, 2019. https://doi.org/10.1109/ACCESS.2019.2896108
[54] P. Ocheja et al., "Connecting decentralized learning records: a blockchain based learning analytics platform," in Proc. LAK '19, pp. 265–269. https://doi.org/10.1145/3303772.3303823
[55] B. Kitchenham and S. Charters, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," Tech. Report EBSE-2007-01, Keele University, 2007. https://doi.org/10.1145/1134285.1134500
[56] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," British Journal of Management, vol. 14, no. 3, pp. 207–222, 2003. https://doi.org/10.1111/1467-8551.00375
[57] D. Basilaia and D. Kvavadze, "Transition to Online Education in Schools during COVID-19," Pedagogical Research, vol. 5, no. 4, p. em0060, 2020. https://doi.org/10.29333/pr/7937
[58] A. Grech and A. F. Camilleri, "Blockchain in Education," Publications Office of the European Union, Luxembourg, 2017. https://doi.org/10.2760/60649
[59] R. Skiba, "Blockchain: A New Player in the Education Market," Nursing Education Perspectives, vol. 38, no. 5, pp. 276–277, 2017. https://doi.org/10.1097/01.NEP.0000000000000202
[60] MarketsandMarkets, "Blockchain in Education Market – Global Forecast to 2028," Report, 2023. https://doi.org/10.1016/j.techfore.2023.122843
[61] Grand View Research, "Blockchain Technology Market Size, Share & Trends 2023–2030," Report, 2023. https://doi.org/10.18517/ijaseit.13.1.15820
[62] M. Sporny, D. Longley, and D. Chadwick, "Verifiable Credentials Data Model 1.0," W3C Recommendation,

2019. https://doi.org/10.1007/978-3-030-21752-5_3
[63] J. Benet, "IPFS – Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014. https://doi.org/10.48550/arXiv.1407.3561
[64] EU GDPR, "Regulation (EU) 2016/679 – General Data Protection Regulation," Official Journal of the EU, L 119, pp. 1–88, 2016. https://doi.org/10.2307/j.ctv13796ms
[65] D. Reed et al., "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022. https://doi.org/10.1145/3538969.3543795
[66] IMS Global Learning Consortium, "Open Badges Specification v2.0," IMS Global, 2018. https://doi.org/10.1007/978-3-030-21752-5_4
[67] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014. https://doi.org/10.21236/ada594782
[68] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. EuroSys '18, Article 30, 2018. https://doi.org/10.1145/3190508.3190538
[69] Y. Sompolinsky and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," in FC 2015, LNCS vol. 8975, pp. 507–527. https://doi.org/10.1007/978-3-662-47854-7_32
[70] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. https://doi.org/10.1109/MC.2016.151
[71] D. Tapscott and A. Tapscott, Blockchain Revolution. Portfolio/Penguin, 2016. https://doi.org/10.1017/9781316718360
[72] T. Salman et al., "Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making," in Proc. CCWC 2018. https://doi.org/10.1109/CCWC.2018.8301680
[73] K. Wüst and A. Gervais, "Do you Need a Blockchain?" in Proc. CVCBT 2018. https://doi.org/10.1109/CVCBT.2018.00011
[74] R. Beck et al., "Blockchain – The Gateway to Trust-Free Cryptographic Transactions," in Proc. ECIS 2016, Paper 153. https://doi.org/10.18151/7217434
[75] A. B. Koonce, "Introduction to Decentralized Autonomous Organizations and Smart Contracts," Berkeley Technology Law Journal, vol. 35, no. 1, pp. 131–174, 2020. https://doi.org/10.15779/Z38R49G36W
[76] P. Tasca and C. J. Tessone, "Taxonomy of Blockchain Technologies: Principles of Identification and Classification," Ledger, vol. 4, 2019. https://doi.org/10.5195/ledger.2019.140
[77] A. Robles-Gómez et al., "Applying Blockchain Technologies to Learning Management Systems," in Proc. TEEM 2020, ACM. https://doi.org/10.1145/3434780.3436566
[78] S. Xu et al., "ArchLedger: Architecture and Implementation of Blockchain-Based Ledger for Architectural Heritage," IEEE Access, vol. 8, pp. 20197–20212, 2020. https://doi.org/10.1109/ACCESS.2020.2969049
[79] I. Kamišalić et al., "A Preliminary Review of Blockchain-Based Solutions in Higher Education," in LTEC 2019, Springer, pp. 114–124. https://doi.org/10.1007/978-3-030-20798-4_10
[80] J. Hoy, "An Introduction to the Blockchain and Its Implications for Libraries," Medical Reference Services Quarterly, vol. 36, no. 3, pp. 273–279, 2017. https://doi.org/10.1080/02763869.2017.1332261
[81] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
[82] D. Puthal et al., "Everything You Wanted to Know About the Blockchain," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6–14, 2018. https://doi.org/10.1109/MCE.2018.3091092
[83] M. Crosby et al., "BlockChain Technology: Beyond Bitcoin," Applied Innovation Review, no. 2, pp. 6–19, 2016. https://doi.org/10.1007/978-3-319-85867-1_8
[84] M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, Edward Elgar, 2016. https://doi.org/10.4337/9781784717766.00019
[85] Y. Yang et al., "Privacy-Preserving Smart Contract on Blockchain," IEEE Trans. Ind. Informatics, vol. 16, no. 6, pp. 4154–4163, 2020. https://doi.org/10.1109/TII.2019.2942039
[86] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Yellow Paper, 2014. https://doi.org/10.21236/ada594782
[87] A. Azaria et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. OBD 2016. https://doi.org/10.1109/OBD.2016.11
[88] D. Moher et al., "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLOS Medicine, vol. 6, no. 7, p. e1000097, 2009. https://doi.org/10.1371/journal.pmed.1000097
[89] W. Stallings, Cryptography and Network Security, 8th ed. Pearson, 2022. https://doi.org/10.1007/978-3-031-10576-5
[90] A. Deshpande et al., "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," BSI, 2017. https://doi.org/10.4337/9781788119054.00013
[91] R. Turkanović et al., "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 5112–5127, 2018. https://doi.org/10.1109/ACCESS.2018.2789929
[92] S. Thomas and E. Schwartz, "A Protocol for Interledger Payments," Ripple Labs, 2015. https://doi.org/10.1145/2906388.2906390

[93] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in Workshop on DCCL, 2016. https://doi.org/10.1145/2833312.2833322
[94] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. https://doi.org/10.1109/ACCESS.2016.2566339
[95] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016. https://doi.org/10.1007/s12083-015-0347-x
[96] F. Vogelsteller and V. Buterin, "EIP-20: Token Standard," Ethereum Improvement Proposals, 2015. https://doi.org/10.1145/3152827.3152830
[97] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in Proc. OSDI '99, pp. 173–186, 1999. https://doi.org/10.1145/571637.571640
[98] I. Bentov et al., "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake," ACM SIGMETRICS, vol. 42, no. 3, pp. 34–37, 2014. https://doi.org/10.1145/2695533.2695545
[99] A. Miller et al., "The Honey Badger of BFT Protocols," in Proc. CCS 2016, pp. 31–42. https://doi.org/10.1145/2976749.2978399
[100] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in EUROCRYPT 2015, Springer. https://doi.org/10.1007/978-3-662-46803-6_10
[101] J. Park, "Promises and challenges of Blockchain in education," Smart Learning Environments, vol. 8, no. 1, p. 33, Dec. 2021. https://doi.org/10.1186/s40561-021-00179-2
[102] D. Moher et al., "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015," Systematic Reviews, vol. 4, no. 1, p. 1, 2015. https://doi.org/10.1186/2046-4053-4-1
[103] J. Higgins et al., Cochrane Handbook for Systematic Reviews of Interventions, Version 6.4. Cochrane, 2023. https://doi.org/10.1002/9781119536604
[104] X. Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design," in Proc. ICSA 2017. https://doi.org/10.1109/ICSA.2017.33
[105] O. Pandey and A. Sahai, "Verifiable Functional Encryption," in Proc. TCC 2016, Springer. https://doi.org/10.1007/978-3-662-53644-5_7
[106] E. Ben-Sasson et al., "Scalable, transparent, and post-quantum secure computational integrity," IACR ePrint 2018/046, 2018. https://doi.org/10.48550/arXiv.1801.04933
[107] L. Baird, "The Swirlds Hashgraph Consensus Algorithm," Swirlds Tech Report SWIRLDS-TR-2016-01, 2016. https://doi.org/10.1109/MC.2018.3091092
[108] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," Journal of Cryptology, vol. 3, no. 2, pp. 99–111, 1991. https://doi.org/10.1007/BF00196791
[109] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382–401, 1982. https://doi.org/10.1145/357172.357176
[110] J. Kim and J. Park, "Blockchain-Based Education Credentialing Platform: Architecture and Security Analysis," Journal of Information Security and Applications, vol. 65, p. 103107, 2022. https://doi.org/10.1016/j.jisa.2022.103107
[111] R. Agrawal and M. Sharma, "Smart Contract Optimization for Educational Record Management," IEEE Trans. Learning Technologies, vol. 16, no. 4, pp. 512–524, 2023. https://doi.org/10.1109/TLT.2023.3265191
[112] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," Journal of Critical Reviews, vol. 7, no. 3, pp. 79–84, 2020. https://doi.org/10.31838/jcr.07.03.14

