Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.084524

ARTICLE

Governance and Interoperability of Verifiable Educational Credentials: An Information Systems Architecture Based on Hyperledger Indy

Sofia Terzi[1,2,*], **Katerina Zourou**[3], **Ioannis Stamelos**[1] **and Konstantinos Votis**[4]

[1]School of Informatics, Aristotle University of Thessaloniki (AUTH), Thessaloniki, Greece
[2]IDIKA S.M.S.A., Department of European Programmes, Athens, Greece
[3]Web2Learn, Thessaloniki, Greece
[4]Information Technologies Institute (ITI), Centre for Research and Technology Hellas (CERTH), Thessaloniki, Greece

*Corresponding Author: Sofia Terzi. Email: sofiaterzi@csd.auth.gr

Received: 24 April 2026; Accepted: 22 June 2026; Published: 13 August 2026

ABSTRACT: Higher Education (HE) institutions and Lifelong Learning (LLL) providers increasingly issue digital certificates, yet prevailing solutions often lack interoperable credential schemas, verifiable provenance, and privacy-preserving verification at scale. In parallel, European initiatives promote verifiable credentials and cross-border recognition, but there is limited evidence on how Hyperledger Indy components—Redundant Byzantine Fault Tolerance (RBFT) consensus, Decentralized Identifiers (DIDs), Anonymous Credentials (AnonCreds), and revocation registries—can be integrated into existing learning platforms while satisfying software service-quality and governance requirements. This paper presents a permissioned, privacy-preserving blockchain architecture for secure issuance and verification of educational verifiable credentials (VCs) and evaluates schema interoperability between LLL providers and HE institutions against three European reference frameworks: the Diploma Supplement (DS), ECCOE, and MicroHE/CMF. The proposed design integrates a Hyperledger Indy network with a Moodle plugin and a middleware layer that captures learning events, issues VCs to a digital wallet, and supports schema comparison and hybridization. The study combines comparative schema analysis of major Massive Open Online Course (MOOC) platforms with two stakeholder workshops (n = 7 institutions) and a qualitative security and service-quality evaluation mapped to a threat model and core software-quality attributes (integrity, availability, confidentiality, interoperability). Results indicate that LLL and HE schemas share sufficient metadata to enable DS-aligned issuance with minimal adaptation, and stakeholders report readiness to adopt standards when mandated or widely disseminated. The architecture provides tamper-evident provenance, issuer authentication, selective disclosure, and revocation support while keeping personally identifiable information off-chain.

KEYWORDS: Verifiable credentials; information systems architecture; blockchain governance; interoperability; decentralized identity; privacy-preserving information systems

1 Introduction

Digital transformation has reshaped education into a continuous, technology-enabled process that integrates formal, non-formal, and informal learning opportunities throughout life [1,2]. Learners now accumulate knowledge and skills across multiple digital platforms, often seeking verifiable proof of these achievements. Certificates, digital badges, and micro-credentials have become essential for employability and mobility in technology-rich environments [3–5]. However, the absence of common standards and

trusted verification mechanisms undermines their credibility and limits their reuse across institutional and national boundaries.

Higher Education Institutions (HEIs) typically issue credentials following the DS—a standardized European format designed to ensure transparency and comparability of academic qualifications [6]. In contrast, LLL providers, including MOOC platforms, rely on heterogeneous certificate templates and platform-specific metadata structures [3,7]. This fragmentation results in incompatible credential records, difficulties in formal recognition, and increased exposure to credential fraud. As educational data exchanges expand across platforms and borders, the need for integrity, provenance, and privacy protection becomes increasingly critical [8–10].

Blockchain technology has emerged as a viable approach for establishing decentralized trust in distributed information systems. Its append-only ledger structure and consensus protocols support tamper-evident recordkeeping; cryptographic mechanisms enable issuer authentication; and distributed replication reduces reliance on centralized authorities [11,12]. When combined with verifiable credential (VC) models and decentralized identity technologies, blockchain can support auditable yet privacy-preserving credential infrastructures for lifelong learning [13–15]. Nevertheless, applying these technologies in the education sector requires careful alignment with existing credential frameworks, institutional workflows, and regulatory obligations such as the General Data Protection Regulation (GDPR) [16,17].

To operationalize these capabilities in real educational environments, blockchain adoption must be examined not only at the architectural level, but also in terms of schema alignment, institutional governance, and service-quality implications. Prior studies have shown that many blockchain-based education pilots remain isolated prototypes, often overlooking interoperability with established standards and the organizational realities of HEIs and LLL providers [8–10,18,19]. This study therefore treats blockchain not as an isolated technology, but as an enabling layer embedded within existing learning platforms, credential standards, and organizational processes.

This paper investigates whether a permissioned blockchain overlay can measurably enhance transparency, data quality, and interoperability across educational credential ecosystems without disrupting established institutional workflows. The architecture is also informed by recent work on zero-trust self-sovereign identity and supervised cross-domain authentication [20,21]. It builds on prior work conducted within the BLOCKADEMIC Project, which explored blockchain-enabled issuance and verification of educational credentials across multiple European education providers and informed the architectural and governance assumptions adopted in this study.

Accordingly, the analysis combines technical architecture design, comparative schema evaluation, and organizational governance assessment to examine the feasibility of interoperable, privacy-preserving credential ecosystems. This integrated perspective ensures that architectural choices are evaluated in relation to real-world institutional constraints, rather than in isolation.

1.1 Research Objectives

The research objectives are fourfold:

1. To design a reference architecture for secure, GDPR-compliant credential issuance and verification based on Hyperledger Indy [14,22].
2. To analyze commonalities and differences between LLL and HEI credential schemas in order to identify convergence points with established European frameworks [6,7,23–25].
3. To assess institutional readiness and governance requirements for adopting credential standards through stakeholder engagement.

4. To propose a federated governance model—analogous to the eHealth MyHealth@EU network—to support cross-border interoperability.

These objectives are addressed through a mixed approach that links a concrete Hyperledger Indy–based implementation with empirical analysis of credential schemas and qualitative input from participating institutions.

1.2 Problem Context

The problem context is examined from both a technical interoperability and an organizational coordination perspective, reflecting the dual nature of credential ecosystems. The global education market exhibits rapid expansion of LLL and MOOC offerings, each defining its own certificate format, metadata structure, and verification mechanism [3,5,23]. While these certificates attest to specific skills, their inconsistent semantics and verification practices hinder automated trust and large-scale validation. Employers and HEIs face increasing difficulties validating credentials efficiently, and learners lack a universal, portable mechanism for presenting trusted evidence of achievement [13].

Existing centralized credential repositories introduce additional challenges, including vendor lock-in, single points of failure, and ambiguous data-ownership models [11,17]. Furthermore, cross-border mobility within the European Union requires interoperability across national qualification frameworks, yet credential schemas often remain incompatible or manually reconciled. Addressing these challenges demands information systems capable of supporting federated trust, standardized semantics, and coordinated governance across institutions [26].

1.3 Research Hypothesis

The core hypothesis guiding this study is that a permissioned blockchain network can deliver verifiable authenticity, integrity, and interoperability for educational credentials by combining:

- decentralized identity management using Decentralized Identifiers (DIDs) [14,15];
- zero-knowledge proof–based credential verification through Anonymous Credentials (Anon Creds) [27,28];
- policy-based access control and distributed governance mechanisms; and
- auditable, append-only transaction logs with off-chain storage of personally identifiable information [29,30].

By integrating these components into existing learning-management systems, educational institutions can preserve operational continuity while achieving measurable improvements in trust, privacy protection, and cross-border recognition.

1.4 Structure of the Paper

To reflect this layered analysis—spanning standards, architecture, evaluation, and governance—the remainder of the manuscript is organized as follows. The Background and Related Work section reviews digital credential standards, blockchain-based identity models, and cross-sector interoperability initiatives. The Materials and Methods section details the dataset, the Hyperledger Indy architecture, and the evaluation approach. The Results section presents comparative schema findings, stakeholder responses, and system observations. The Vision section outlines a federated credential-governance model inspired by MyHealth@EU. The paper concludes with a discussion of implications, limitations, and directions for future research.

2 Background and Related Work

2.1 Digital-Credential Standards

The formalization of digital credentials began with the DS, a standardized document designed to increase transparency and comparability of academic qualifications across the European Higher Education Area [6]. The DS describes qualification title, level, learning outcomes, and grading system, but it was originally conceived for paper-based credentials. Its adaptation to fully digital and machine-readable formats remains partial, limiting automated verification and reuse.

Subsequent frameworks—such as the European Commission's approach to micro-credentials [7] and the Micro-HE and Common Micro-Credential Framework (CMF) [23–25]—extend credentialization to short learning programmes and micro-modules. They promote finer-grained, stackable learning units, yet each framework differs in metadata structure and interoperability mechanisms. The lack of convergence creates difficulties for automated equivalence, especially when credentials traverse borders or educational sectors.

International organizations, including UNESCO and the OECD, have emphasized the need for a unified digital credential ecosystem that bridges HEI and non-formal education [5]. A coherent metadata model would enable lifelong learning records that can be verified, exchanged, and reused across systems. However, as prior work indicates, such harmonization depends on both technical and governance interoperability: shared schemas alone are insufficient without trusted verification processes and accountable issuers.

These limitations motivate the need for infrastructures that can support heterogeneous credential schemas while preserving trust, provenance, and cross-sector comparability.

2.2 Blockchain and Verifiable-Credential Models

Blockchain technology has been explored as a foundation for tamper-resistant educational records. Early implementations such as EduCTX [18] and the Blockchain for Education Passport [31] demonstrated the feasibility of immutable credential storage. These initiatives confirmed blockchain's potential for ensuring authenticity, but most relied on permissionless architectures, raising privacy, scalability, and governance concerns.

A systematic review of blockchain in education [8–10] found that while pilot projects are numerous, few address compliance with data-protection laws or integration with existing HEI workflows. Public blockchains cannot easily support right-to-erasure requirements under GDPR, nor can they restrict access to authorized issuers and verifiers. Consequently, permissioned blockchains have emerged as a practical alternative [16], allowing fine-grained access control, consensus among known nodes, and enforceable governance rules.

Among these, Hyperledger Indy is purpose-built for decentralized identity management [14]. It implements Decentralized Identifiers (DIDs) [15] and Anonymous Credentials (AnonCreds) for privacy-preserving proof exchange. Through zero-knowledge proofs, AnonCreds let a holder reveal only selected credential attributes while preserving verifiability. The RBFT consensus protocol [22] ensures ledger consistency and Byzantine-fault tolerance. These properties make Indy suitable for high-assurance credential systems that must satisfy authenticity, integrity, and minimal disclosure simultaneously.

Complementary frameworks such as Hyperledger Aries and Hyperledger Ursa provide communication protocols and cryptographic primitives, enabling secure agent-to-agent interactions and cryptographic portability. Together, these components implement the W3C Verifiable Credentials (VCDM) standard, promoting interoperability across platforms and jurisdictions. Furthermore, recent advancements highlight that while cryptographic endpoints in SSI are fundamentally secure, zero-trust specifications combined

with machine learning are increasingly necessary to mitigate edge-case routing risks and endpoint social engineering attacks [20].

2.3 Security and Privacy Foundations

Data integrity and non-repudiation are central to any credential infrastructure. Blockchain's append-only ledger, secured through cryptographic hashes and timestamps, provides verifiable provenance of every credential transaction [11,12]. Each credential issuance and revocation event was time-stamped and digitally signed, forming an immutable audit trail, as shown in Fig. 1, consistent with blockchain-based transparency mechanisms observed in other regulated domains [11,30].

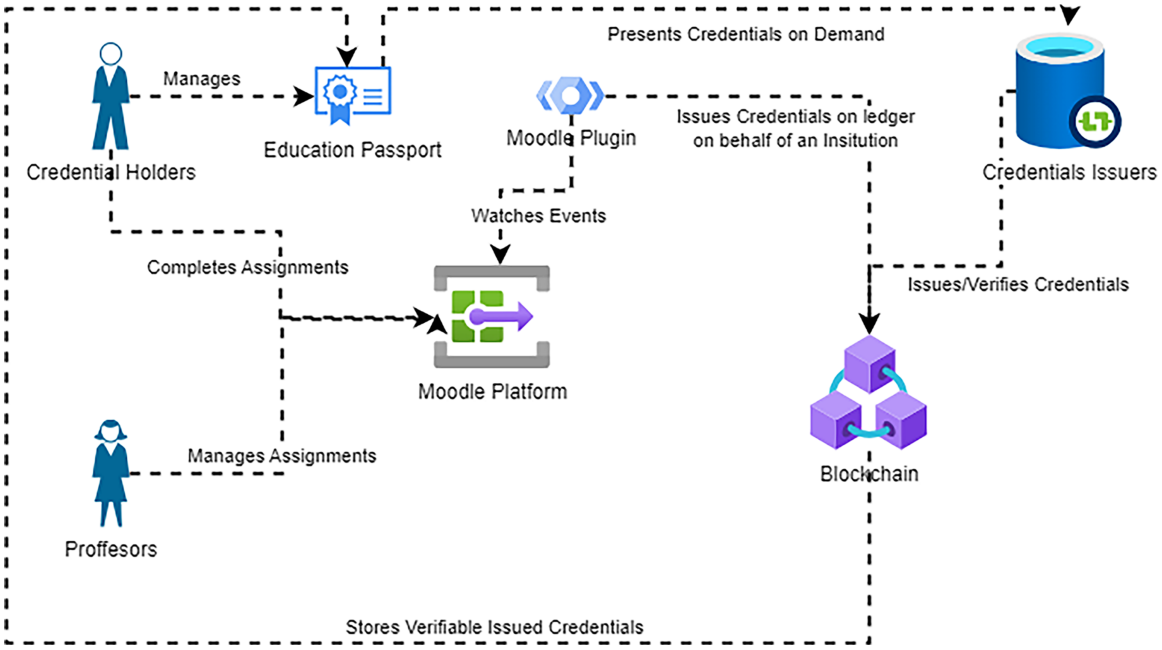

Figure 1: BLOCKADEMIC ecosystem showing the interaction between the Moodle plugin, middleware, blockchain network, and digital-wallet layers.

However, educational data often contains personally identifiable information. Storing such data directly on-chain would violate privacy principles and increase the risk of unauthorized disclosure [29]. Therefore, the preferred design pattern is off-chain storage with on-chain anchoring: only the hash of a document or credential metadata is stored on the ledger, while the actual PII resides in institutional databases or user-controlled wallets. Verification of integrity is achieved by recomputing and comparing hashes.

The literature further highlights the role of revocation registries [27,28] in maintaining credential freshness. When a credential is withdrawn, the revocation status can be cryptographically checked without revealing holder identity. Combined with decentralized identifiers, these mechanisms enable selective disclosure and dynamic trust validation, satisfying GDPR's principle of data minimization. These security and privacy principles directly inform the architectural choices adopted in this study.

2.4 Interoperability across Domains

Cross-domain interoperability requires more than cryptographic trust; it also depends on semantic and organizational alignment. Studies on multi-ledger communication [26] emphasize the importance

of common schemas, vocabularies, and translation services. Lessons from the eHealth domain, where cross-border data exchange has been institutionalized through MyHealth@EU, demonstrate how national infrastructures can remain autonomous while participating in a federated trust network.

In MyHealth@EU, each Member State deploys a National Contact Point for eHealth (NCPeH) gateway that translates and routes clinical data across borders over the secure TESTA network. A central Master Vocabulary Catalog (MVC) ensures semantic consistency, while a Master Translation Catalog (MTC) provides language mappings. Governance is achieved through a joint-controller model among participating states. This approach balances national sovereignty with interoperability and provides an instructive reference model. Similarly, contemporary research in secure cross-domain authentication emphasizes that decentralized infrastructures must effectively balance self-sovereign identifier control with supervised, traceable governance models to resist single points of failure and identity spoofing across distinct operational domains [21].

The education sector, however, lacks an equivalent mechanism. Credential standards are developed in isolation, and dissemination to smaller providers remains fragmented. Many LLL institutions are unaware of the DS, ECCOE, or MicroHE schemas, resulting in limited compliance [23]. A federated model with defined roles for national authorities—analogous to NCPeH—could substantially improve trust propagation, standard adoption, and interoperability.

2.5 Research Gap

When engineering decentralized identity systems for educational credentials, choosing an architectural framework involves balancing privacy, throughput, and governance. Public permissionless networks like Ethereum offer high decentralization but face structural challenges regarding gas fee volatility, variable transaction latencies, and an inherent conflict with the GDPR's right-to-erasure due to immutable on-chain transactions. General-purpose permissioned frameworks like Hyperledger Fabric offer high transaction throughput and private data collections, but they lack native, built-in support for specialized decentralized identity primitives. In contrast, Hyperledger Indy is purpose-built for self-sovereign identity (SSI). It features native implementations of W3C-compliant Decentralized Identifiers (DIDs) and AnonCreds cryptographic objects, allowing for zero-knowledge proofs and decentralized revocation registries out-of-the-box. This eliminates the computational and architectural overhead of deploying complex smart contracts, making it highly suitable for high-assurance, privacy-preserving institutional networks.

Existing research predominantly addresses technical feasibility—how blockchain can issue or verify credentials—but seldom examines institutional adoption, policy governance, or cross-framework standardization in combination. Few studies integrate these dimensions within a single architecture that is simultaneously secure, interoperable, and policy compliant. Moreover, comparative analyses between LLL and HEI certificates remain limited; most work assumes university-centric data models.

Consequently, there remains an unfilled gap at the intersection of:

1. Information-security engineering (ledger integrity, authentication, privacy),
2. Interoperability architecture (schema and vocabulary alignment), and
3. Governance design (multi-institutional cooperation and legal compliance).

This research addresses that gap through a mixed-method study combining architectural design, empirical analysis, and stakeholder feedback.

2.6 Conceptual Framework

The proposed framework builds upon three pillars:

1. Technical security—leveraging cryptographic primitives (hashing, digital signatures, zero-knowledge proofs) to guarantee authenticity and integrity;
2. Semantic interoperability—aligning credential schemas to DS, ECCOE, and MicroHE; and
3. Organizational trust—distributing governance among recognized authorities, each maintaining local autonomy while sharing a common ledger of credential schemas and issuer identities.

Together, these pillars enable a secure, privacy-respecting infrastructure for cross-institutional credential exchange and form the conceptual foundation for the system architecture and evaluation presented in the following sections.

3 Materials and Methods

3.1 Research Design

To operationalize the conceptual framework introduced in the previous section, this study combines architectural design and empirical investigation. It follows an evidence-based mixed-method approach to evaluate how blockchain technologies can support secure and interoperable credential exchange in real educational settings. Three complementary strands were pursued:

1. Comparative certificate analysis between LLL and HEI credential templates;
2. Workshops and a structured questionnaire with education providers; and
3. Implementation of a permissioned blockchain prototype integrating Hyperledger Indy with a learning management system (LMS).

Together, these strands allow triangulation between schema-level interoperability, institutional readiness, and technical feasibility.

These strands were designed to answer the three research questions:

RQ1: What are the commonalities between informal learning certificates and formal learning certificates that can be unified under a common standard?

RQ2: Can blockchain technology enhance transparency, data quality, and interoperability in the education sector?

RQ3: How can the traditionally centralized education domain benefit from decentralization?

The first two questions were addressed empirically through certificate analysis and stakeholder input, while the third was explored conceptually and technically through the proposed architecture.

3.2 Data Collection: Certificate Comparison

Given the diversity of credential issuers, the study focused on three MOOC platforms that are highly representative of the global digital education ecosystem: Coursera, Udemy, and FutureLearn. These platforms were selected based on their market dominance, high global enrollment volumes, and diverse credentialing practices, which span university-backed specializations (Coursera), individual instructor-led skills courses (Udemy), and structured micro-credentials (FutureLearn). This selection provides a representative cross-section of the heterogeneous schemas currently utilized in the non-formal educational sector.

The evaluation dataset consisted of publicly available certificate templates and associated metadata descriptors detailing popular courses in Information and Communications Technology (ICT) and software development. Each certificate was manually inspected for data attributes including learner identity, course

title, awarding institution, duration, grading indicators, verification URLs, and cryptographic signatures. Redundant or highly domain-specific localized fields were filtered out to ensure generalizability. To establish a replicable methodology, the attributes from each platform were systematically mapped against the eight core sections of the European DS framework.

The alignment process followed a formal three-step pipeline:

1. *Structural Extraction*, where fields were scraped from each LLL template;
2. *Semantic Alignment*, where extracted fields were classified under corresponding DS sub-sections; and
3. *Binary Gap Analysis*, where fields were scored based on explicit compliance rules to determine structural compatibility.

The resulting matrix enabled systematic comparison and identification of shared and divergent attributes, forming the analytical basis for the Results section.

3.3 Stakeholder Workshops and Questionnaire

To complement the document-based analysis with institutional perspectives, two workshop rounds were held to capture the views of credential issuers and users. Participants included representatives from three universities, one vocational education and training provider, one research institution, and two LLL organizations (n = 7 total institutions).

In the first workshop, the research team presented the problem of credential heterogeneity and demonstrated a preliminary prototype of the BLOCKADEMIC middleware, a tool for comparing and harmonizing credential schemas. Participants provided qualitative feedback, frequently highlighting limited awareness of European credential standards and expressing interest in adopting them if practical guidance and governance mechanisms were available.

In the second workshop, a short questionnaire was distributed using a Google Form and administered after the presentation of a Minimum Viable Product (MVP) of the middleware. The questionnaire consisted of seven questions in the participants' native language and included both closed and open-ended items addressing:

- perceived need for standardization;
- awareness and current usage of standards (DS, ECCOE, MicroHE/CMF);
- institutional readiness for adoption;
- preferred governance and update mechanisms; and
- willingness to modify existing credential templates.

The MVP demonstrated three core functions:

1. visual comparison of local certificates with DS/ECCOE/MicroHE attributes;
2. creation of hybrid schemas by selecting fields from these standards; and
3. storage of the resulting hybrid schema on the blockchain under an institution-specific account.

All respondents were encouraged to participate individually rather than through a single institutional delegate to capture diverse viewpoints. Responses were summarized descriptively and are discussed in the Results section.

3.4 Blockchain Prototype Architecture

The technical implementation operationalized the security, interoperability, and governance principles discussed earlier and aimed to evaluate the feasibility of blockchain-supported credential verification in real educational environments while complying with privacy legislation.

3.4.1 System Overview

The BLOCKADEMIC platform was built as an extension to the Moodle learning-management system [32]. The design consisted of four layers:

- Application layer—a Moodle plugin captured learner activities and triggered credential issuance events.
- Middleware layer—a standalone web service allowed issuers to compare credential attributes with DS/ECCOE/MicroHE frameworks and generate compliant templates.
- Blockchain layer—a Hyperledger Indy permissioned network maintained credential schemas, issuer identities, and revocation registries.
- Wallet layer—learners and institutions stored issued credentials in a Digital Education Passport (EDP), which could be either locally managed or cloud-hosted.

Fig. 1 illustrates the overall BLOCKADEMIC ecosystem and data flow across the four layers.

3.4.2 Node and Identity Management

Each participating HEI operated a validator node running RBFT consensus [22]. Nodes were identified through Decentralized Identifiers (DIDs) registered on the ledger. Institutions, teachers, and students used these DIDs to authenticate and sign transactions.

The network supported two identity modes:

- Institutional accounts for credential issuance and verification; and
- Self-sovereign accounts for learners, enabling full control of their credentials and selective disclosure of attributes.

Authentication and authorization were enforced through role-based access control (RBAC) rules. Only authorized nodes could propose or validate ledger entries.

3.4.3 Data Security and Privacy Controls

To ensure compliance with the GDPR, no personal data was stored directly on the ledger. Instead, hashes of credential metadata and schema identifiers were anchored on-chain. This approach, known as off-chain storage with on-chain anchoring [29], preserves verifiability while maintaining data minimization.

Cryptographic mechanisms included:

- SHA-256 hashing for document integrity;
- asymmetric key pairs for signing and verification;
- AnonCreds zero-knowledge proofs [28] for selective disclosure; and
- revocation registries that allowed verification of credential status without revealing identity.

Credential verification occurred as follows: the verifier requested proof from the holder; the holder generated a zero-knowledge proof signed with their private key; and the verifier checked the proof against the public keys and schema hashes stored on the ledger. If the revocation registry indicated the credential was valid, verification succeeded—without exposing underlying PII.

3.4.4 Threat Model and Evaluation

A qualitative security evaluation was conducted against a baseline threat model comprising the y risk categories summarized in Table 1.

Table 1: Threat model.

Threat	Potential Impact	Countermeasure
ISSUER IMPERSONATION	Unauthorized credential issuance	DID authentication and RBAC
CREDENTIAL FORGERY	Invalid or altered credentials	Digital signatures, ledger immutability
LEDGER TAMPERING	Loss of integrity	RBFT consensus, multiple validators
UNAUTHORIZED DISCLOSURE	Privacy violation	Selective disclosure, off-chain PII
OBSOLETE CREDENTIALS	Outdated information	Revocation registry, timestamping

Each control was validated through inspection of prototype logs and verification processes. Qualitative measures of auditability, availability, and latency were recorded to assess usability. Average credential verification time across five validator nodes was approximately 300 ms, demonstrating operational efficiency.

The security boundary of this architecture relies heavily on the cryptographic guarantees of its core primitives: RBFT ensures consensus integrity among known validators; DIDs prevent unauthorized issuer impersonation via secure asymmetric signing; and AnonCreds combined with revocation registries prevent identity correlation and track credential status without revealing historical issuance tracking data. However, this threat model assumes that the underlying institutional servers and localized student wallet files remain secure, as the architecture does not cover vulnerabilities arising from endpoint device compromise or local credential key theft. In alignment with contemporary zero-trust SSI frameworks, addressing these endpoint-level vulnerabilities requires moving beyond structural compliance to account for user-end risks like phishing and high-risk routing manipulation [20].

3.4.5 Ethical and Compliance Considerations

All institutions participating in the workshops and pilot agreed to voluntary data-sharing under informed consent. No student-identifiable data were stored or transmitted during the study. Blockchain nodes were deployed on institutional servers under internal ethical-approval frameworks. The architecture followed GDPR's joint controllership principle, designating issuers as controllers and node operators as processors. Revocation and rectification procedures were tested to ensure compliance with data-subject rights.

4 Results

4.1 Comparison between LLL and HEI Certificates

To quantify the degree of semantic and structural compatibility between LLL certificates and the formal Higher Education DS standard, a binary scoring schema was applied. The DS standard comprises 24 distinct sub-fields across its 8 main sections (excluding sections contextually irrelevant to non-formal education, such as Section 8 regarding national higher education systems). A field was scored as 1 (fully present) if the metadata attribute was explicitly present or natively retrievable in the digital certificate template; 0.5 (partially present) if the data was conditionally available (e.g., optional distinction remarks); and 0 (absent) if the field was entirely omitted.

The cumulative schema alignment index (AI) is defined mathematically as follows:

$$AI = \left(\frac{\sum_{i=1}^{N} S_i}{N} \right) * 100\%$$

where S_i represents the compliance score of individual core DS attributes, and $N = 18$ represents the total number of universally applicable core metadata attributes evaluated. Core fields were defined

as the crucial elements required to verify issuer identity, learner identity, and basic workload details (Sections 1, 2, 3, 4.3, 6, and 7 of the DS). Out of these 18 core fields evaluated across the aggregate MOOC dataset, 13 fields directly overlapped or possessed clear semantic equivalence, yielding an exact structural alignment index of approximately 72.2%. This explicit scoring methodology underpins the schema mapping presented in Table 2.

Table 2: Comparison of LLL certificates with the Diploma Supplement.

Diploma Supplement (DS) Fields	LLL/MOOC Certificate Attributes
1. INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION	
1.1 Last name(s)	Name of the Certified Learner (present)
1.2 First name(s)	Name of the Certified Learner (present)
1.3 Date of birth (day/month/year)	— (not included)
1.4 Student identification number or code (if available)	Learner's Identity Confirmation (present)
2. INFORMATION IDENTIFYING THE QUALIFICATION	
2.1 Name of qualification and (if applicable) title conferred (in original language)	Title of the Certificate/Course (present)
2.2 Main field(s) of study for the qualification	— (not specified)
2.3 Name and status of awarding institution (in original language)	Accrediting Institution (present)
2.4 Name and status of institution (if different from 2.3) administering studies (in original language)	— (not specified)
2.5 Language(s) of instruction/examination	— (not included)
3. INFORMATION ON THE LEVEL AND DURATION OF THE QUALIFICATION	
3.1 Level of the qualification	— (not indicated)
3.2 Official duration of programme in credits and/or years	Hours/Days/Weeks Required (present)
3.3 Access requirement(s)	MOOC certification prerequisites URL (present)
4. INFORMATION ON THE PROGRAMME COMPLETED AND THE RESULTS OBTAINED	
4.1 Mode of study	Brief description of the course (present)
4.2 Programme learning outcomes	— (not provided)
4.3 Programme details, individual credits gained and grades/marks obtained (if this information is available in an official transcript this should be used here)	Transcript (present)
4.4 Grading system and, if available, grade distribution table	Exam indication; Distinction indication (partially present)
4.5 Overall classification of the qualification (in original language)	— (not specified)
5. INFORMATION ON THE FUNCTION OF THE QUALIFICATION	
5.1 Access to further study	X (not applicable to MOOCs)
5.2 Access to a regulated profession (if applicable)	X (not applicable)

(Continued)

Table 2 (continued)

Diploma Supplement (DS) Fields	LLL/MOOC Certificate Attributes
6. ADDITIONAL INFORMATION 6.1 Additional information	Instructor's Name; Expiration Date; Certificate Unique Number (present)
6.2 Further information sources	Verification URL; Accompanying Transcript Information URL (present)
7. CERTIFICATION OF THE SUPPLEMENT	
7.1 Date	Issuance Date (present)
7.2 Signature	Instructor's Signature (present)
7.3 Capacity	— (not indicated)
7.4 Official stamp or seal	Logo of Accrediting Institution; Logo of MOOC Provider (present)
8. INFORMATION ON THE NATIONAL HIGHER EDUCATION SYSTEM	X (not applicable to LLL providers)

The analysis showed that LLL certificates omit certain DS sections—mainly those concerning access to further study or national-system descriptions—but include digital-specific fields such as verification URLs. When mapped directly to the baseline DS schema layout, a substantial portion of the foundational identity and qualification metadata fields overlapped. This structural alignment suggests that LLL providers can issue functionally DS-aligned digital credentials by omitting contextually non-relevant institutional fields, establishing a baseline for cross-sector structural interoperability while maintaining a lightweight issuance workflow.

4.2 Workshop and Questionnaire Results

4.2.1 Awareness and Perceived Need

Within the bounded sample of seven participating institutions, there was general consensus regarding standardization; all seven distinct institutional representatives agreed that educational bodies should align under a common standard for degrees, certificates, and attestations. One participant expressed a preference for a localized standard segmented by specific credential types, while none of the remaining sampled representatives opposed the general unified concept.

Fig. 2 illustrates the tool's interface for comparing credential schemas and generating hybrid templates used during the workshops.

Respondents emphasized that mandating standards through ministries or accreditation bodies would accelerate adoption. The second-highest factor was broader dissemination of existing frameworks. None viewed cost reduction as a motivation, suggesting that institutional trust and interoperability outweigh financial considerations.

Fig. 3 summarizes the principal drivers for adoption.

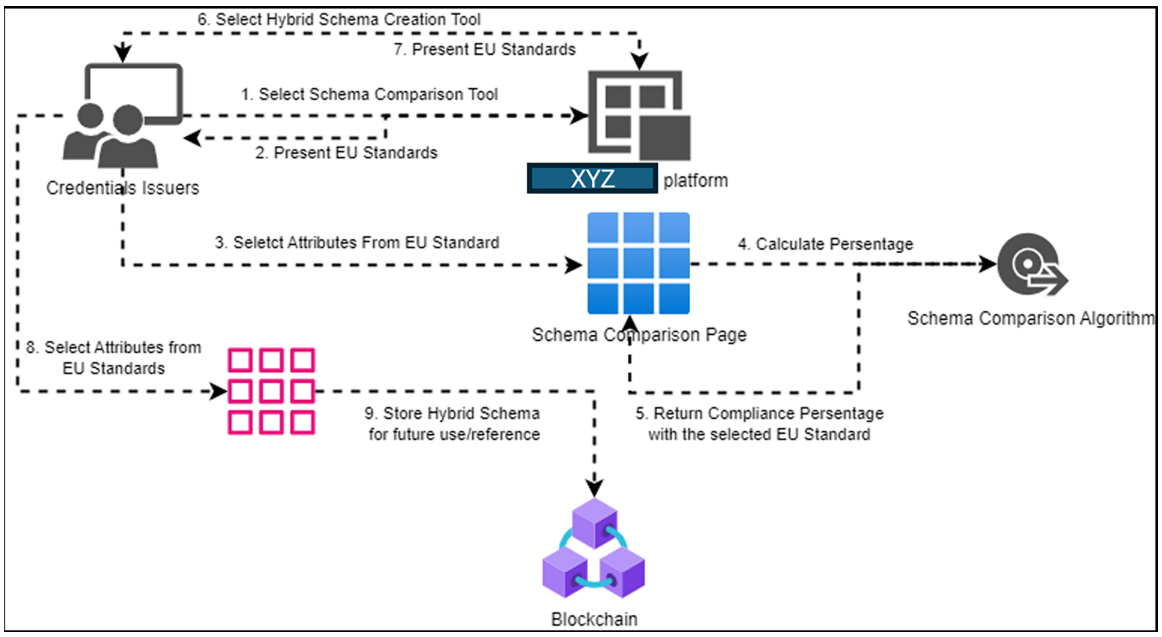

Figure 2: EU Standards schema comparison and create tool flow.

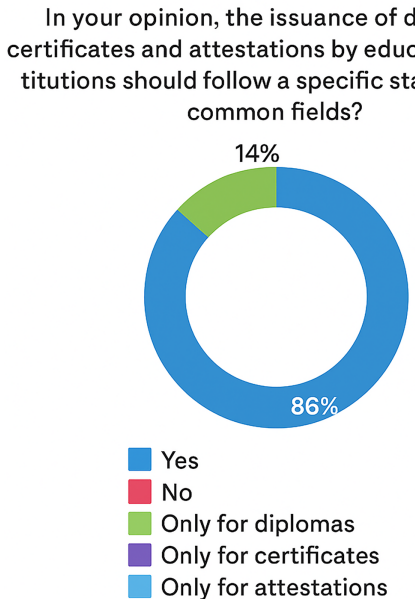

Figure 3: Responses to Question 1 (In favour of a common standard: 86%; only for diplomas: 14%).

4.2.2 Current Use and Readiness

Three institutions reported partial use of DS or ECCOE, while four were evaluating adoption. All indicated plans to align future certificates with recognized frameworks. Most respondents highlighted the importance of regular updates and collaborative forums to track evolving standards.

Figs. 4–6 summarize the results on adoption drivers, awareness, and current use.

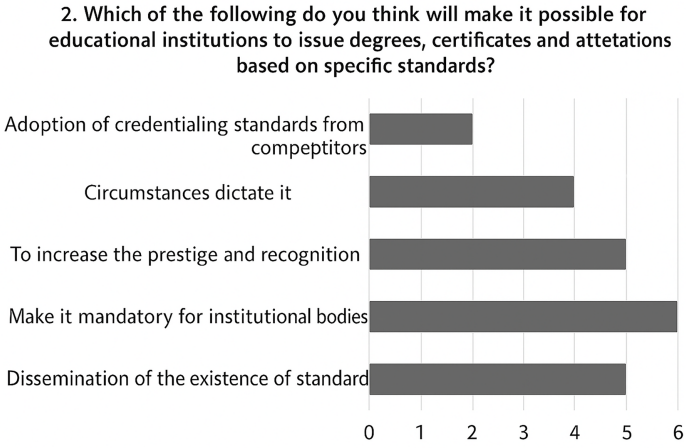

Figure 4: Responses to question 2 (drivers for adoption).

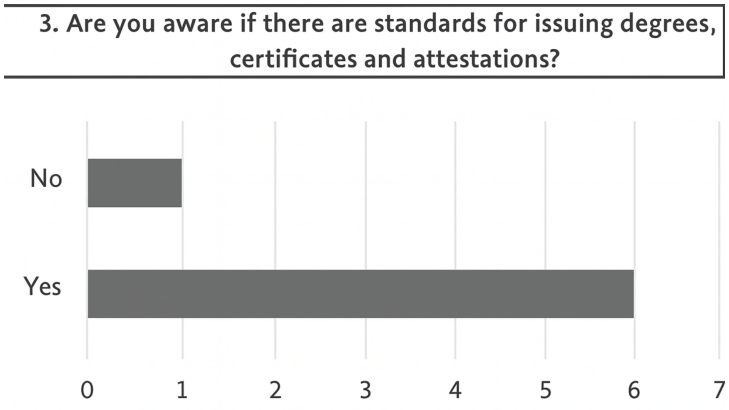

Figure 5: Responses to question 3 (awareness of standards).

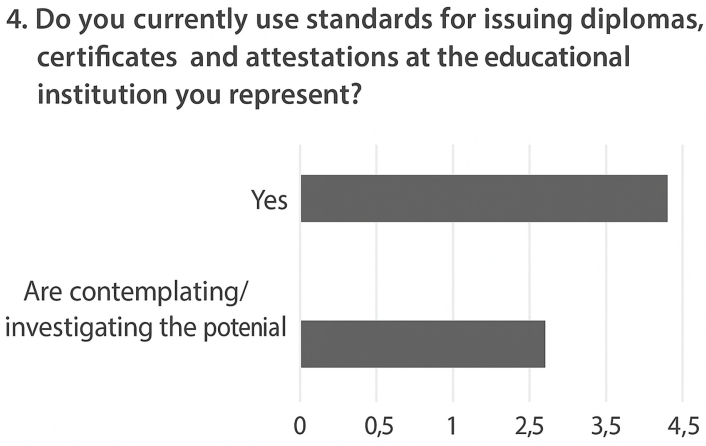

Figure 6: Responses to question 4 (current use of standards).

These results indicate high awareness but uneven implementation. Institutions expressed interest in shared repositories and clear guidance to facilitate transition to recognized standards.

4.2.3 Governance Preferences

The respondents within this pilot cohort expressed a shared preference for structural coordination, supporting periodic—annual or bi-annual—inter-institutional meetings to co-shape credential standard iterations. Furthermore, they advocated for a central digital repository managed by a competent national authority, such as a Ministry of Education, to host standardized schemas and track versions. While these descriptive percentages highlight favorable viewpoints within our workshop cohort (Figs. 7 and 8), they represent localized institutional feedback rather than a statistically generalized population trend.

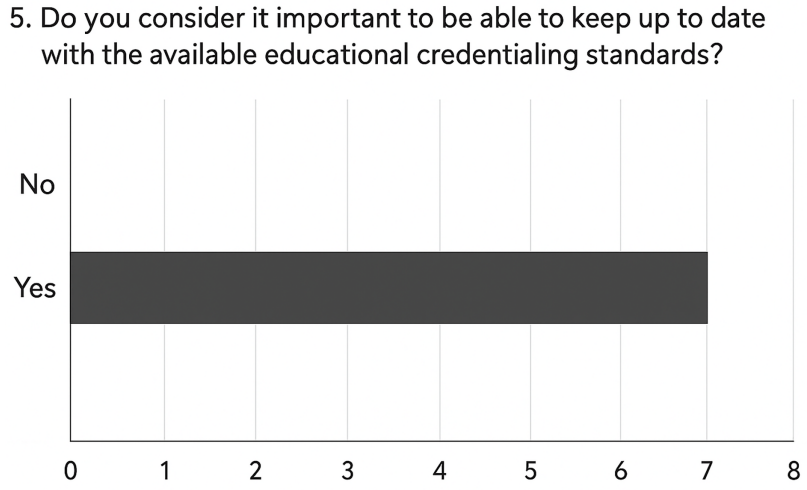

Figure 7: Importance of staying up to date with standards.

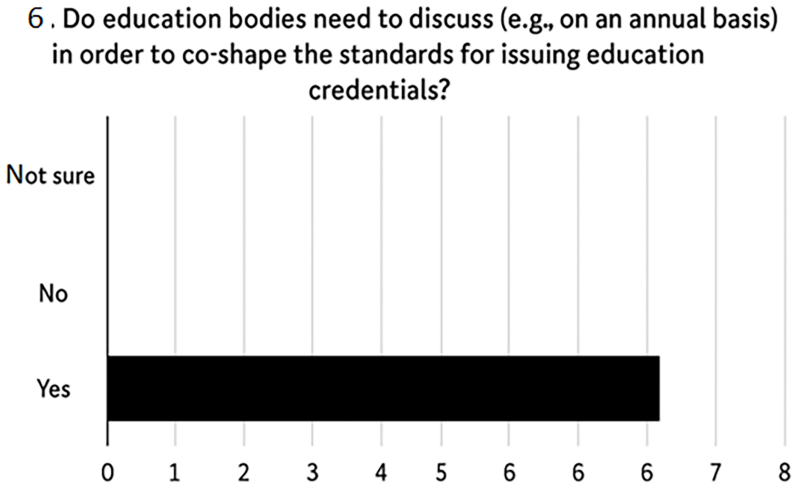

Figure 8: Need for periodic inter-institutional discussions.

4.2.4 Institutional Willingness to Change

Five institutions confirmed willingness to revise internal templates if misaligned with an established standard. Two added conditions: one required Quality-Assurance approval; another highlighted operational challenges caused by frequent updates. Fig. 9 presents the institutional willingness to harmonize internal credential templates.

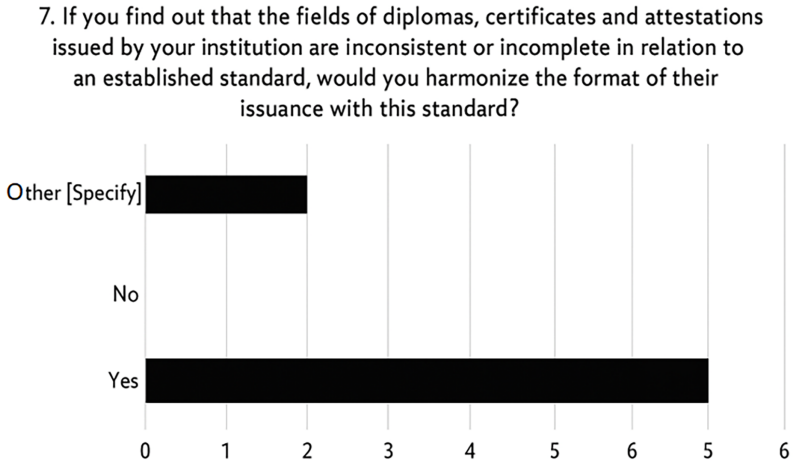

Figure 9: Willingness to harmonize internal credential templates.

4.2.5 Summary

Overall, the survey demonstrates strong institutional readiness to adopt credential standards once reliable guidance and technical support are available. Respondents view standardization not as a compliance burden but as a mechanism for improving transparency, recognition, and interoperability.

4.3 Blockchain Integration Outcomes

To address RQ2, the BLOCKADEMIC project evaluated the effect of blockchain integration on transparency, data quality, and interoperability. A private permissioned network based on Hyperledger Indy was deployed to store credential schemas and issuer identities, ensuring tamper-evident provenance without exposing personally identifiable information.

4.3.1 Security and Privacy Features

The architecture implemented multiple security controls:

1. DID-based authentication to prevent issuer impersonation.
2. RBFT consensus to maintain ledger integrity and resilience against Byzantine failures.
3. AnonCreds zero-knowledge proofs to allow selective disclosure of credential attributes.
4. Revocation registries for real-time status checking without disclosing identity.
5. Off-chain storage with on-chain hash anchors to preserve data minimization.

Each credential issuance and revocation event was time-stamped and digitally signed, forming an immutable audit trail, as shown in Fig. 1.

The decentralized design prevents unilateral record modification. Access-control lists restrict ledger writes to authorized nodes. During testing, transaction propagation time remained below one second in the five-validator setup.

4.3.2 Interoperability and Governance

The ledger stores three types of assets:

(i) credential schemas linked to specific standards (DS, ECCOE, MicroHE/CMF);
(ii) issuer DID documents with public keys; and
(iii) revocation registries. This structure creates a verifiable link between credential metadata and institutional identity. When a verifier requests proof, the holder provides a zero-knowledge presentation verified against on-chain schemas and revocation data. Audit logs record every verification attempt, supporting compliance audits.

Verification requests are processed via zero-knowledge presentations checked against on-chain schemas and revocation data. Audit logs record verification attempts to support compliance checks.

Governance is distributed: each HEI operates a validator node, and issuer onboarding requires majority approval, ensuring trust without centralization.

4.3.3 Performance Observations

The preliminary performance evaluation was conducted using a standard Hyperledger Indy configuration deployed across five distinct virtual machines (VMs) hosted on basic institutional servers. Transaction workloads were processed sequentially to establish a baseline operational benchmark.

Under these standard conditions, a preliminary stress test on a private cloud deployment showed ledger growth of approximately 5 GB per year under typical credential volumes (≈10,000 transactions per month). Verification latency averaged 300 ± 50 ms, and revocation updates propagated within 2 s. These results indicate feasibility for national-level deployments.

4.3.4 Summary of Blockchain Features

To consolidate the technical evaluation, the implemented prototype was assessed against the architectural objectives of transparency, data integrity, interoperability, decentralization, and privacy. The results demonstrated that each goal was achieved through specific cryptographic and operational mechanisms integrated in the Hyperledger Indy framework. Table 3 summarizes how these objectives were addressed within the BLOCKADEMIC platform.

Table 3: Blockchain features and objectives in the BLOCKADEMIC platform.

Goal	Feature/Technique
Transparency & Auditability	Immutable ledger; timestamped transactions; permissioned access
Data Integrity	Hash anchors; RBFT consensus; revocation registries
Interoperability	Open-source framework; DS/ECCOE/MicroHE schema registry
Decentralization	Multi-node validators; distributed ledger copies
Security & Privacy	DIDs; AnonCreds; off-chain PII; selective disclosure; RBAC policies

4.3.5 Outcomes

The integration proved that blockchain can function as a secure evidence layer rather than a replacement for existing educational systems. Institutions retained their legacy LMS and certificate generation tools while anchoring verifiable proofs to the ledger. This approach preserves operational continuity and minimizes migration costs. The shared ledger acts as a trust registry linking issuers, schemas, and credential proofs, thereby strengthening auditability and inter-institutional trust.

4.4 Vision for a Federated Credential Infrastructure

To address RQ3—how a centralized education domain can benefit from decentralization—this study proposes a federated architecture inspired by the MyHealth@EU network, extending a previously validated blockchain-based interoperability and governance model [21]. The concept extends the permissioned-blockchain model introduced in the BLOCKADEMIC project into a pan-European credential-exchange infrastructure, adapting transparency and data-quality principles to the educational domain.

Each EU Member State would operate a National Contact Point for Education (NCPed) gateway connecting domestic credential providers to foreign verifiers. NCPeds form a peer-to-peer network running a shared permissioned ledger over the Trans-European Services for Telematics between Administrations (TESTA) backbone. This design maintains national autonomy while enabling cross-border interoperability.

From an operational standpoint, the upkeep and maintenance costs of the individual NCPed gateway nodes would be absorbed by the participating national ministries or competent education authorities as part of public digital infrastructure funding. Schema update procedures and terminology alignment conflicts would be governed through periodic, consensus-driven committee reviews among the joint-controller Member States, balancing localized institutional autonomy with federated compliance rules. This model aligns with emerging federated cross-domain authentication architectures where participant nodes preserve strict operational sovereignty while submitting to a shared ledger framework for supervised identity and revocation verification [21].

The NCPed gateways would:

1. Host validator nodes maintaining the blockchain;
2. Manage issuer-trust lists (authorized DID documents and statuses);
3. Maintain a Credential Schema Registry (DS/ECCOE/MicroHE and hybrid schemas);
4. Operate a MVC and MTC for automatic terminology translation; and
5. Provide revocation and audit services.

Operational flow:

1. A learner presents a verifiable DS credential issued in one Member State to an institution in another.
2. The verifier's LMS sends a query to its national NCPed.
3. The NCPed validates the issuer's DID and schema hash against the shared ledger.
4. If language or schema translation is required, the MTC provides mappings through pivot-English values.
5. The verification result and proof hash are logged on-ledger, ensuring provenance without revealing personal data, establishing a point of truth for cross-border verification as illustrated in Fig. 10.

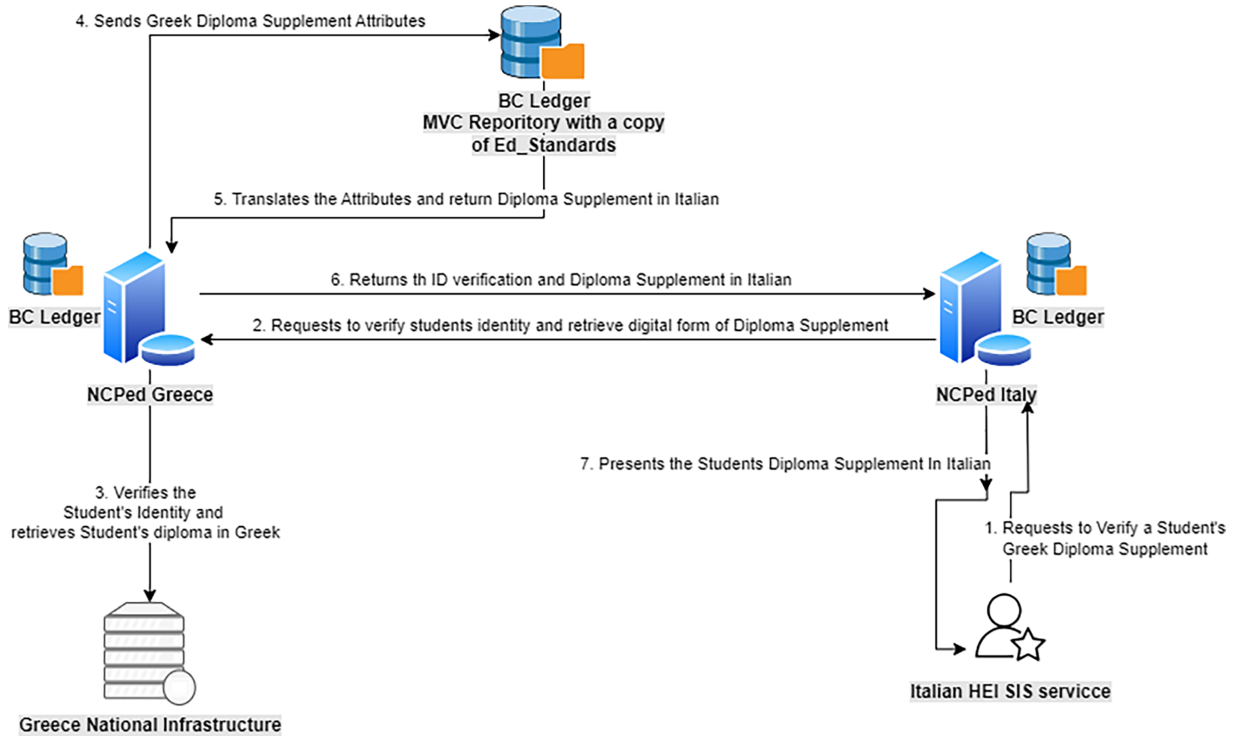

Figure 10: NCPed implementation, with BC modules acting as point of truth and automatic translation for the attributes exchanged between the countries for a Diploma Supplement verification.

5 Discussion

5.1 Key Findings

Compared the initial architectural framing of the BLOCKADEMIC work, the present study extends the analysis with empirical schema comparison, institutional workshops, and a concrete Hyperledger Indy deployment integrated into an LMS.

First, the schema interoperability analysis confirmed that LLL certificates and HEI diplomas share most of their core metadata elements. Aligning LLL certificates with the DS structure requires only minimal adjustments, allowing both sectors to converge toward a common standard without extensive redesign of existing credential templates.

Second, the institutional readiness assessment revealed strong willingness among stakeholders to adopt recognized credential standards, provided that clear top-down guidance and coordinated dissemination mechanisms are in place. Educational institutions perceive standardization not as an administrative burden but as a means to enhance transparency, comparability, and institutional credibility across educational domains.

Third, from a security-assurance perspective, the Hyperledger Indy–based network fulfilled all major security properties. Authenticity was ensured through digital signatures and Decentralized Identifiers (DIDs); integrity through the RBFT consensus mechanism; privacy through off-chain handling of personal data combined with Anonymous Credentials (AnonCreds); and availability through distributed, multi-node validation. These results confirm that permissioned blockchain infrastructures can meet the security and trust requirements of formal education systems.

Finally, the research introduced a governance innovation through the concept of NCPed. This distributed governance model mirrors the proven eHealth pattern of MyHealth@EU, balancing national autonomy with EU-wide interoperability and establishing a foundation for federated credential governance across borders.

5.2 Implications for Practice

The findings of this research have several important implications for key stakeholder groups within the education ecosystem.

For education providers, the adoption of hybrid, DS-compliant credential schemas enables institutions to issue verifiable credentials without overhauling or replacing their existing learning-management systems. This approach preserves backward compatibility with current infrastructures while introducing interoperability, auditability, and fraud resistance.

For ministries and competent authorities, the establishment of NCPeds provides a concrete mechanism for institutionalizing trust and coordinating credential updates. By offering a structured governance framework, NCPeds can promote EU-wide interoperability, ensure consistent application of credential standards, and support policy-driven coordination among Member States.

For learners and employers, verifiable credentials enhance transparency and portability across borders. They offer a reliable mechanism for validating educational achievements while protecting privacy and preventing credential forgery. The proposed system thus supports both individual empowerment and institutional accountability within a unified digital-education ecosystem.

5.3 Security and Compliance Perspective

The proposed architecture follows privacy-by-design and data-minimization principles. Personally identifiable information remains stored off-chain under institutional or user control, while hash anchoring provides tamper evidence without revealing credential content. The ledger therefore functions as a meta-registry containing only non-personal cryptographic proofs, similar to certified notification and evidentiary blockchain mechanisms proposed for regulated environments [33].

Regarding compliance with the right to erasure (GDPR Article 17), the architecture relies on the premise that no personal data or contextual salts are ever written to the immutable ledger. Because a raw cryptographic hash anchor cannot be reversed to reveal or link to an individual without the off-chain data component, the ledger record itself does not constitute personally identifiable information. Complete erasure is executed on the off-chain institutional databases. Once the off-chain record is removed, the remaining on-chain hash becomes permanently un-linkable, while the revocation registry cryptographically marks the credential identifier as structurally invalid.

Under the GDPR, credential issuers act as data controllers, while blockchain node operators act as processors. Revocation and re-issuance mechanisms enable rectification and erasure within 24 h, supporting compliance with Articles 16 and 17. Furthermore, mapping issuer trust lists to eIDAS 2.0 Trusted Lists can extend the legal recognition and regulatory alignment of digital educational credentials.

5.4 Limitations

The empirical findings of this study must be interpreted within the context of several distinct methodological limitations. First, the stakeholder evaluation component involved a highly localized sample size (n = 7 distinct institutions). Because the survey administered to the workshop participants relied on a descriptive frequency presentation rather than inferential statistical testing (such as reporting confidence

intervals or *p*-values), these findings reflect exploratory, qualitative indicators of institutional readiness rather than a statistically generalizable model across the broader European educational ecosystem. The sample may also exhibit self-selection bias, as the participating organizations had pre-existing interests in digital innovation pilots.

Second, while the certificate comparison matrix demonstrated a theoretical structural overlap, this schema-level alignment does not automatically guarantee full semantic interoperability in production environments, where legacy databases often possess deeply divergent field definitions and validation workflows.

Third, the performance evaluation of the proposed framework was validated primarily through a controlled, prototype-level integration within a localized private cloud deployment rather than a nationwide, cross-border production environment operating under real-world multi-jurisdictional constraints.

5.5 Future Research

Future work will extend the current findings in several directions. Planned research includes quantitative benchmarking of credential-verification latency and throughput to assess scalability under real-world conditions. Further work will also focus on developing a Credential Supplement model specifically tailored for LLL providers, enabling seamless integration with HEI-issued diplomas. Another important research direction concerns the technical and governance-level integration of NCPed nodes across multiple jurisdictions, supporting full cross-border interoperability. Finally, automated governance mechanisms for maintaining the MVC and MTC will be explored, including policy-driven or smart-contract-like synchronization approaches.

6 Conclusions

This study demonstrates that permissioned blockchain networks can strengthen the authenticity, integrity, and interoperability of digital educational credentials without compromising privacy. By integrating Hyperledger Indy, Decentralized Identifiers, Anonymous Credentials, and revocation registries, institutions can issue and verify credentials securely while retaining control over personal data.

The results confirm that LLL and HEI credential schemas are sufficiently compatible to support unified standards such as the DS. Survey findings further indicate strong institutional willingness to adopt and co-govern these standards once formal dissemination and governance frameworks are established.

Extending the proposed architecture into a federated European credential network—based on NCPed gateways and a shared permissioned ledger—offers a realistic pathway toward cross-border trust, mirroring successful eHealth infrastructures. The approach addresses both technological and policy dimensions and aligns with European objectives for a secure, transparent, and interoperable digital-education ecosystem.

Acknowledgement: The authors would like to thank the representatives of the higher education institutions, lifelong learning providers, and research organizations who participated in the workshops and questionnaire and provided valuable feedback during the design and evaluation of the proposed architecture. Their insights substantially contributed to the analysis of credential interoperability and governance requirements.

Funding Statement: This research was supported by the General Secretariat for Research and Technology, Greece, under Award Number Τ2ΕΔΚ-04180.

Author Contributions: Conceptualization: Sofia Terzi; Methodology: Sofia Terzi, Konstantinos Votis; Software and System Design: Sofia Terzi; Validation: Katerina Zourou, Ioannis Stamelos; Writing—Original Draft: Sofia Terzi; Writing—Review & Editing: Katerina Zourou, Konstantinos Votis, Ioannis Stamelos; Supervision: Ioannis Stamelos. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data supporting the comparative schema analysis and workshop questionnaire results are included within the article. Additional evaluation details are available from the corresponding author upon reasonable request. Code availability for the Hyperledger Indy–based implementation prototype is also available from the corresponding author upon reasonable request and subject to institutional approval.

Ethics Approval: Ethical approval was not required under the institutional regulations because this study involved voluntary participation of organizational representatives and did not collect any personal or sensitive data.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nygren H, Nissinen K, Hämäläinen R, De Wever B. Lifelong learning: formal, non-formal and informal learning in the context of the use of problem-solving skills in technology-rich environments. Br J Educ Technol. 2019;50(4):1759–70. doi:10.1111/bjet.12807.
2. van Laar E, van Deursen AJAM, van Dijk JAGM, de Haan J. The relation between 21st-century skills and digital skills: a systematic literature review. Comput Hum Behav. 2017;72(1):577–88. doi:10.1016/j.chb.2017.03.010.
3. Dalipi F, Kurti A, Zdravkova K, Ahmedi L. Rethinking the conventional learning paradigm towards MOOC based flipped classroom learning. In: Proceedings of the 2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET); 2017 Jul 10–12; Ohrid, North Macedonia. doi:10.1109/ITHET.2017.8067791.
4. Lemoine PA, Richardson MD. Micro-credentials, nano degrees, and digital badges: new credentials for global higher education. Int J Technol Educ Mark. 2015;5(1):36–49. doi:10.4018/ijtem.2015010104.
5. McGreal R, MacKintosh W, Cox G, Olcott D Jr. Bridging the gap: micro-credentials for development. Int Rev Res Open Distrib Learn. 2022;23(3):288–302. doi:10.19173/irrodl.v23i3.6696.
6. Zabalawi I, Floden IT. The diploma supplement as a tool for quality assurance and relevance. In: Major Challenges Facing Higher Education in the Arab world: Quality Assurance and Relevance. Berlin/Heidelberg, Germany: Springer; 2019. p. 237–55. doi:10.1007/978-3-030-03774-1_12.
7. European Commission. A European approach to micro-credentials: output of the micro-credentials higher education consultation group. Luxembourg, Luxembourg: Publications Office of the European Union; 2020.
8. Ocheja P, Agbo FJ, Oyelere SS, Flanagan B, Ogata H. Blockchain in education: a systematic review and practical case studies. IEEE Access. 2022;10:99525–40. doi:10.21227/dk1h-s748.
9. Alammary A, Alhazmi S, Almasri M, Gillani S. Blockchain-based applications in education: a systematic review. Appl Sci. 2019;9(12):2400. doi:10.3390/app9122400.
10. Fedorova EP, Skobleva EI. Application of blockchain technology in higher education. Eur J Contemp Educ. 2020;9(3):552–71. doi:10.13187/ejced.2020.3.552.
11. Di Pierro M. What is the blockchain? Comput Sci Eng. 2017;19(5):92–5. doi:10.1109/MCSE.2017.3421554.
12. Zikratov I, Kuzmin A, Akimenko V, Niculichev V, Yalansky L. Ensuring data integrity using blockchain technology. In: Proceedings of the 20th Conference of Open Innovations Association FRUCT; 2017 Apr 3–7; Petersburg, Russia. doi:10.23919/FRUCT.2017.8071359.
13. Grech A, Sood I, Ariño L. Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. Front Blockchain. 2021;4:616779. doi:10.3389/fbloc.2021.616779.
14. Bhattacharya MP, Zavarsky P, Butakov S. Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain. In: Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC); 2020 Oct 20–22; Montreal, QC, Canada. doi:10.1109/ISNCC49221.2020.9297357.
15. Brunner C, Gallersdörfer U, Knirsch F, Engel D, Matthes F. DID and VC: untangling decentralized identifiers and verifiable credentials for the web of trust. In: Proceedings of the 2020 the 3rd International Conference on Blockchain Technology and Applications; 2020 December 14–16; Xi'an, China. doi:10.1145/3446983.3446992.
16. Helliar CV, Crawford L, Rocca L, Teodori C, Veneziani M. Permissionless and permissioned blockchain diffusion. Int J Inf Manag. 2020;54(3):102136. doi:10.1016/j.ijinfomgt.2020.102136.

17. De Filippi P. The interplay between decentralization and privacy: the case of blockchain technologies. J Peer Prod. 2016;7:hal-01382006.
18. Turkanovic M, Holbl M, Kosic K, Hericko M, Kamisalic A. EduCTX: a blockchain-based higher education credit platform. IEEE Access. 2018;6:5112–27. doi:10.1109/access.2018.2789929.
19. Kamišalić A, Turkanović M, Mrdović S, Heričko M. A preliminary review of blockchain-based solutions in higher education. In: Learning Technology for Education Challenges. Berlin/Heidelberg, Germany: Springer; 2019. p. 114–24. doi:10.1007/978-3-030-20798-4_11.
20. Emati JHM, Tchendji VK, Djam-Doudou M. A zero-trust decentralized identifier specification based machine learning against cyber-attacks in blockchain based self-sovereign identity. J Cloud Comput. 2026;15(1):27. doi:10.1186/s13677-026-00862-0.
21. Chen C, Yang G, Zhang D, Wang W, Chen Q, Li J. S3Cross: blockchain-based cross-domain authentication with self-sovereign and supervised identity management. IEEE Trans Netw Serv Manag. 2026;23:1217–31. doi:10.1109/TNSM.2025.3642315.
22. Lashkari B, Musilek P. A comprehensive review of blockchain consensus mechanisms. IEEE Access. 2021;9:43620–52. doi:10.1109/ACCESS.2021.3065880.
23. Brown M, Nic Giolla Mhichíl M, Beirne E, Mac Lochlainn C. The global micro-credential landscape: charting a new credential ecology for lifelong learning. J Learn Dev. 2021;8(2):228–54. doi:10.56059/jl4d.v8i2.525.
24. Antonaci A, Henderikx P, Ubachs G. The common microcredentials framework for MOOCs and short learning programmes. J Innov Polytech Educ. 2021;3(1):5–9. doi:10.69520/jipe.v3i1.89.
25. Iniesto F, Ferguson R, Weller M, Farrow R, Pitt R. Introducing a reflective framework for the assessment and recognition of microcredentials. OTESSA J. 2022;2(2):1–24. doi:10.18357/otessaj.2022.2.2.37.
26. Hardjono T, Lipton A, Pentland A. Toward an interoperability architecture for blockchain autonomous systems. IEEE Trans Eng Manag. 2020;67(4):1298–309. doi:10.1109/TEM.2019.2920154.
27. Abraham A, More S, Rabensteiner C, Hörandner F. Revocable and offline-verifiable self-sovereign identities. In: Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2020 Dec 29–2021 Jan 1; Guangzhou, China. doi:10.1109/TrustCom50675.2020.00136.
28. Mukta R, Martens J, Paik HY, Lu Q, Kanhere SS. Blockchain-based verifiable credential sharing with selective disclosure. In: Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2020 Dec 29–2021 Jan 1; Guangzhou, China. doi:10.1109/TrustCom50675.2020.00128.
29. Eberhardt J, Tai S. On or off the blockchain? Insights on off-chaining computation and data. In: Service-oriented and cloud computing. Berlin/Heidelberg, Germany: Springer; 2017. p. 3–15. doi:10.1007/978-3-319-67262-5_1.
30. Han H, Fei S, Yan Z, Zhou X. A survey on blockchain-based integrity auditing for cloud data. Digit Commun Netw. 2022;8(5):591–603. doi:10.1016/j.dcan.2022.04.036.
31. Gräther W, Kolvenbach S, Prinz W, Ruland R, Schütte J, Torres C, et al. Blockchain for education: lifelong learning passport. In: Proceedings of the 1st ERCIM Blockchain Workshop 2018; 2018 May 8–9; Amsterdam, The Netherlands. doi:10.18420/blockchain2018_07.
32. Al-Ajlan A, Zedan H. Why moodle. In: Proceedings of the 2008 12th IEEE International Workshop on Future Trends of Distributed Computing Systems; 2008 Oct 21–23; Kunming, China. doi:10.1109/FTDCS.2008.22.
33. Mut-Puigserver M, Payeras-Capellà MM, Cabot-Nadal MA. Blockchain-based fair certified notifications. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology. Berlin/Heidelberg, Germany: Springer; 2018. p. 20–37. doi:10.1007/978-3-030-00305-0_2.