**International Journal of Applied Mathematics**

**Volume 38 No. 7s, 2025**

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# A FORMAL ARCHITECTURE FOR PRIVACY-PRESERVING CREDENTIAL VERIFICATION USING BLOCKCHAIN AND ZERO-KNOWLEDGE PROOFS

**Kadhim Abdulfadhil Gatea[1], Ehsan Shoja[2], Parviz Rashidi-Khazaee[3*], Hossein Nahid-Titkanlou[4]**

[1] Ph.D. Student, Faculty of Electrical and Computer Engineering, Urmia University,

Km 11 Sero Road, Urmia - 5756151818, IRAN (full postal address, in English)

e-mail: k.abdulfadhil@urmia.ac.ir

[2] Assistant Professor, Faculty of Electrical and Computer Engineering, Urmia University,

Km 11 Sero Road, Urmia - 5756151818, IRAN

e-mail: e.shoja@urmia.ac.ir

[3] Assistant Professor, Information Technology and Computer Engineering Department, Urmia University of Technology,

Band Road, 2 km Band Blvd, Urmia - 5716693817, IRAN

e-mail: p.rashidi@uut.ac.ir

[4] Assistant Professor, Department of Industrial Engineering, Payame Noor University,

Nakhl Street, Artesh Boulevard, Tehran - 1955717413, IRAN

e-mail: Hossein_Nahid@pnu.ac.ir

**Abstract**

This paper addresses the challenge of designing secure and private digital credentialing systems by leveraging advanced mathematical primitives from applied cryptography. The core of our proposed solution is the application of Zero-Knowledge Proofs (ZKPs), a class of cryptographic protocols that allows for the verification of assertions without disclosing the underlying secret data. We introduce a formal, layered architecture that demonstrates how the mathematical properties of ZKPs can be systematically translated into a robust, large-scale information system. The framework's design is validated against the complex requirements of the academic domain, which serves as a rigorous testbed for our architectural approach. The primary contribution is a blueprint for integrating complex cryptographic protocols into practical system design, demonstrating how mathematical guarantees of privacy can be preserved in a distributed and verifiable manner. This work provides a novel contribution at the intersection of applied cryptography, system architecture, and information security.

Math. Subj. Classification 2020: 94A60, 68P25, 68M14

Received: August 13 2025

International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

**Keywords:** credential verification, system architecture, blockchain, zero-knowledge proofs, applied cryptography, information systems security, distributed systems.

## 1 Introduction

The global transformation toward remote digital interaction has fundamentally altered the nature of verifiable credentials, evolving them from static documents into dynamic digital assets [1], [2], [3]. This paradigm shift presents multifaceted challenges for any ecosystem—encompassing users, issuing authorities, and verifiers—requiring verification methods that are simultaneously trustworthy, efficient, and secure [4], [5], [6], [7]. Traditional verification systems face an inherent tension between establishing trust and preserving privacy. These systems predominantly rely on direct sharing of sensitive records, thereby exposing users to significant privacy risks while creating compliance challenges for organizations operating under stringent regulations such as the General Data Protection Regulation (GDPR) [8], [9]. Moreover, the vulnerability of conventional systems to fraud and forgery, coupled with escalating rates of cyberattacks, underscores the pressing need for more robust architectural solutions [1], [10], [11].

Blockchain technology has emerged as a compelling foundation for verification systems, leveraging decentralized and immutable ledgers to enhance both security and transparency [12], [13], [14]. Through smart contract implementation, blockchain systems can automate validation processes, substantially reducing administrative burden [11], [15], [16]. However, the inherently public nature of most blockchain architectures introduces a fundamental paradox: the pursuit of data integrity must not compromise user confidentiality—a paramount consideration in any system handling sensitive information [2].

Zero-Knowledge Proofs (ZKPs) offer an elegant cryptographic solution to this dilemma. These protocols enable a credential holder to prove the validity of a specific mathematical statement (e.g., "I possess a required certification") without disclosing ancillary sensitive information (e.g., personal details or performance metrics). This capability intrinsically supports data minimization principles while empowering users with granular control over their personal information. The technical foundations of modern non-interactive ZKPs (e.g., zk-SNARKs) are built upon advanced mathematical constructs such as elliptic curve pairings and polynomial commitment schemes [17], [18]. The synergistic combination of blockchain's immutability and ZKPs' privacy-preserving capabilities presents a pathway toward truly secure and confidential verification systems, grounded in mathematical guarantees [2], [18], [19].

Despite this considerable potential, a critical implementation gap persists. Numerous technology-driven initiatives have failed to achieve widespread adoption, primarily because they neglect the complex interplay between user requirements and regulatory frameworks [20], [21], [22]. These "technology-first" approaches frequently yield systems characterized by poor usability, inadequate compliance with privacy legislation, limited interoperability, and insufficient institutional buy-in—the latter being a crucial prerequisite for successful implementation.



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This research directly addresses this gap by advocating a requirements-driven approach that inverts the conventional design paradigm. Rather than commencing with technological capabilities, our methodology begins with a comprehensive analysis of the operational, security, and regulatory requirements of a high-stakes environment. Informed by this analysis, we introduce a formal architectural framework that strategically employs blockchain and ZKPs as instruments to address identified real-world challenges. Our objective is to bridge the chasm between the theoretical potential of cryptographic protocols and the practical imperatives of a functional and secure information ecosystem. Ultimately, this work provides a comprehensive blueprint for a system that enhances not merely security and efficiency, but fundamentally advances user autonomy over their digital identity.

This paper is organized as follows: Section 2 provides a critical review of emerging credential verification systems. Section 3 delineates our system design methodology. Section 4 presents the proposed architectural framework, elaborating on its design and operational protocols. Section 5 provides a detailed architectural analysis of the framework's technical properties. Section 6 concludes the paper with a synthesis of our contributions, and finally, Section 7 outlines directions for future research.

## 2 Background and Related Work

The verification of digital credentials necessitates a delicate equilibrium among three fundamental system requirements: integrity (ensuring authenticity and tamper-resistance), efficiency (optimizing speed while minimizing computational costs), and privacy (maintaining user sovereignty over personal data). This section critically examines the evolutionary trajectory of verification systems, elucidating how successive technological innovations have addressed specific requirements while inadvertently exposing others, thereby revealing the precise research gap this paper addresses.

### 2.1 Traditional Systems and The First Wave: Blockchain for Integrity

Legacy verification systems—encompassing both paper-based mechanisms and siloed digital databases—exhibit systemic deficiencies that render them inadequate for contemporary digital ecosystems. These systems are characterized by operational inefficiencies, endemic vulnerability to fraud, and a fundamental lack of interoperability required for an increasingly globalized environment [1], [3], [8], [23]. From a systems engineering perspective, three critical shortcomings emerge: (1) an absence of user agency, wherein users possess minimal control over their own data [22], [24]; (2) substantial privacy vulnerabilities arising from excessive data disclosure that frequently contravenes data protection frameworks such as GDPR [20], [25]; and (3) fundamental trust deficits that undermine credential value for all stakeholders [1], [26].

Blockchain technology emerged as a transformative solution to address these integrity and trust challenges. Through its decentralized, immutable ledger architecture, pioneering “first-generation” credentialing platforms (detailed in Table 1) successfully demonstrated that digital credentials could be reliably anchored and verified, establishing cryptographic guarantees of authenticity.


Received: August 13 2025

**International Journal of Applied Mathematics**

**Volume 38 No. 7s, 2025**

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1: Comparative Analysis of Selected Blockchain-Based Credential Verification Systems

| System / Provider | Key Features | Advantages | Limitations |
|---|---|---|---|
| University of Nicosia (https://www.unic.ac.cy) | Issues academic certificates (e.g., diplomas) on the Bitcoin blockchain | Instant verification, enhanced transparency, pioneering adoption model | Primarily institution-focused; requires sustained institutional commitment for broader impact; limited functionality beyond basic certificate issuance |
| Blockcerts Learning Machine / Hyland (https://www.blockcerts.org) | Open-source standard and platform for issuing, viewing, and verifying blockchain-anchored credentials | Promotes interoperability, issuer/recipient sovereignty, vendor-neutral standard | Variable institutional adoption; technical complexity barriers; dependency on compatible wallet infrastructure affecting accessibility |
| Dock Association (https://www.dock.io) | Platform for issuing and verifying W3C Verifiable Credentials using Decentralized Identifiers (DIDs) on dedicated Polkadot parachain | Strong standards alignment (W3C VCs, DIDs), emphasizes user control, leverages modern blockchain infrastructure | Ecosystem dependency on Polkadot; nascent adoption limiting verifier networks; complexity for users unfamiliar with DID/VC paradigms |
| OopenCerts: Governmentof Singapore (https://opencerts.io/) | Government-backed initiative utilizing Ethereum blockchain for national educational | Strong governmental endorsement ensuring high trust levels within Singapore; | Geographic specificity to Singaporean context; Ethereum main net transaction costs; scalability challenges for |



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

| System / Provider | Key Features | Advantages | Limitations |
|---|---|---|---|
| | certificate issuance and verification | open-source framework | international deployment |
| Disciplina.io (https://disciplina.io/) | Connects academia-student-employer triad via blockchain; stores verified achievements for recruitment; employs proprietary blockchain | Facilitates verified data sharing and streamlined recruitment; enhances employer transparency; student-controlled data | Highly reliant on network adoption (institutions & employers); proprietary blockchain may limit interoperability; limited market adoption to date. |

Critical analysis of these platforms reveals a fundamental limitation pervading first-generation implementations. While systems such as OpenCerts effectively address integrity concerns through blockchain-anchored credential hashes, verification protocols still necessitate transmission of complete credential files. This "all-or-nothing" disclosure paradigm, despite securing document integrity, fundamentally violates data minimization principles. The inherent tension between ensuring integrity and preserving confidentiality exposes a critical architectural flaw in first-generation blockchain solutions, establishing the imperative for subsequent technological evolution.

### 2.2 ZKPs for Privacy-Preserving Verification

Zero-Knowledge Proofs (ZKPs) present an elegant cryptographic resolution to this fundamental dilemma. These protocols enable a "prover" (e.g., a user) to convince a "verifier" of a statement's validity without revealing any information beyond the truth of that specific claim [20], [27]. A ZKP system must satisfy three core mathematical properties: completeness (an honest prover can always convince the verifier), soundness (a dishonest prover cannot convince the verifier of a false statement), and zero-knowledge (the verifier learns nothing other than the statement's validity) [2], [19], [27].

The mathematical underpinnings of modern non-interactive ZKPs, particularly zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), are rooted in a multi-stage process that transforms a computational statement into a verifiable, cryptographic proof. This process typically involves three key steps:

Arithmetization: The first step is to convert the computational statement into a formal mathematical representation. The statement to be proven (e.g., "I know a secret input w such that hash(w) equals a public value h") is flattened into a series of basic arithmetic operations



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(addition and multiplication) over a finite field. This representation is known as an arithmetic circuit [2], [18], [28]. The goal is to create a system where the statement is true if and only if there exists a valid set of inputs that satisfy all gates in this circuit.

Polynomial Representation: The arithmetic circuit is then converted into an equivalent representation using polynomials. A common method for this is the Rank-1 Constraint System (R1CS), which transforms each logic gate of the circuit into an equation of the form $(a \cdot s) * (b \cdot s) - (c \cdot s) = 0$, where a, b, and c are vectors and s is the solution vector containing all inputs and intermediate values. The entire computation's validity can then be condensed into a single, large target polynomial, t(x), which is zero at specific points if and only if all constraints are satisfied. The prover's task is now to convince the verifier that they know a set of secret polynomials that satisfy this condition, without revealing the polynomials themselves[2], [28], [29].

Cryptographic Proof Generation: Finally, cryptographic primitives are used to create a short, non-interactive proof. The prover uses techniques like polynomial commitment schemes (e.g., Kate-Zaverucha-Goldberg or KZG) to "commit" to their secret polynomials. These commitments are then combined and verified using cryptographic pairings on elliptic curves. A pairing is a special bilinear map $e: G1 \times G2 \rightarrow GT$ that allows for the verification of certain polynomial equations without revealing the underlying polynomials. The final proof is a small set of elliptic curve points that the verifier can use, along with public parameters, to quickly check the required mathematical relationships. The security of the entire scheme relies on well-established mathematical hardness assumptions, such as the Discrete Logarithm Problem in these groups, ensuring that forging a proof for a false statement is computationally infeasible [28].

This capability empowers users to prove precise assertions (e.g., “I possess a required certification”) while maintaining complete confidentiality over ancillary information, thereby facilitating selective disclosure and establishing genuine data sovereignty [30], [31]. Table 2 demonstrates ZKPs’ versatile applications across various domains.

Table 2: Illustrative Use Cases and Properties of ZKPs

| Use Case | Description / Example | Advantages | Limitations | References |
|---|---|---|---|---|
| Cryptocurrency Transactions | Zcash implementation using zk-SNARKs for shielded transactions | Transaction anonymity; protection of participant identities and transaction amounts | Computational overhead; potential for illicit applications; cryptographic complexity | [32] |
| Identity Management | Decentralized identity | User sovereignty; selective | Standardization challenges; | [31], [33] |



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

| Use Case | Description / Example | Advantages | Limitations | References |
|---|---|---|---|---|
| | systems: Sovrin, Hyperledger Indy | disclosure capabilities; resistance to identity correlation | scalability constraints; user experience complexity | |
| Academic Credential Verification | Proving graduation status without revealing grades or personal coursework details | Selective disclosure; privacy preservation; GDPR compliance; enhanced student empowerment | Computational complexity; absence of standardization; ZKP scheme design intricacies | [4], [30], [34] |
| Financial Qualification | Demonstrating financial eligibility for loans without exposing account details | Financial privacy protection; selective proof generation; discrimination mitigation | Implementation complexity; regulatory compliance challenges; trust establishment | [35] |
| Healthcare Credentialing | Practitioner credential verification systems (e.g., MedRec) | Enhanced patient safety; administrative efficiency; privacy protection | Regulatory complexity; security requirements; interoperability challenges | [36] |
| Anonymous Voting Systems | E-voting platforms: Helios, zkVote | Ballot secrecy; public verifiability; voter anonymity preservation | Scalability limitations; technical infrastructure requirements; usability barriers | [37] |
| Sybil-Resistant Identity | Worldcoin, Humanity Protocol: biometric- | Prevention of duplicate identities; privacy- | Ethical implications of biometric usage; scalability concerns; | [38] |


Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

| Use Case | Description / Example | Advantages | Limitations | References |
|---|---|---|---|---|
| | based proof-of-personhood | preserving verification | hardware dependencies | |
| Government/Cross-Border ID | Estonia e-Residency, EU Digital Identity Wallet | Citizen privacy protection; selective cross-border attribute disclosure | Regulatory fragmentation; implementation complexity; governance challenges | [39], [40] |

Various ZKP schemes (e.g., zk-SNARKs, zk-STARKs, Bulletproofs) present distinct trade-offs concerning proof size, verification speed, and cryptographic assumptions, rendering scheme selection a critical architectural decision. Nevertheless, despite considerable theoretical promise, ZKP adoption within educational contexts remains embryonic, impeded by implementation complexity and absence of standardized protocols [20], [27].

### 2.3 Identifying the Research Gap: Beyond Technology-First Solutions

While blockchain and ZKPs are theoretically well-established technologies, existing implementations reveal a critical gap. Current solutions predominantly adopt technology-first approaches, prioritizing technical sophistication over a principled design grounded in the operational requirements of the target domain. This misalignment produces systems with poor usability, inadequate regulatory compliance, and limited institutional adoption—all essential for meaningful deployment. The missing element is a holistic, requirements-driven architectural framework that prioritizes the real-world needs of users, issuers, and verifiers. This research addresses this gap by proposing a framework grounded in systematic requirements engineering rather than pre-selected technological capabilities. By inverting the conventional design paradigm—from technology-driven to requirements-driven—we can create systems that achieve not only technical robustness but also genuine usability, regulatory compliance, and user empowerment.

## 3 System Design Methodology

Addressing the multifaceted socio-technical challenges inherent in credential verification necessitates an integrative and systematic design methodology. This research employs a structured, iterative design process, common in systems engineering, which is particularly suited for developing innovative solutions to complex problems through cycles of analysis, design, evaluation, and refinement. Our approach is grounded in established principles of requirements engineering and privacy engineering [41].

Our hybrid methodology synthesizes two foundational engineering frameworks:



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **Privacy by Design (PbD):** This framework mandates that privacy considerations be embedded proactively into the system architecture from the outset, rather than being treated as an add-on [42].
- **Systematic Requirements Analysis:** We employ a structured approach to systematically analyze and integrate functional and non-functional requirements from all key actors within the target ecosystem (e.g., users, issuers, verifiers) [43].

This synthesis ensures the resulting framework transcends mere technical novelty to deliver a practical and robust solution. The research progressed through a four-phase process, visualized in Figure 1.

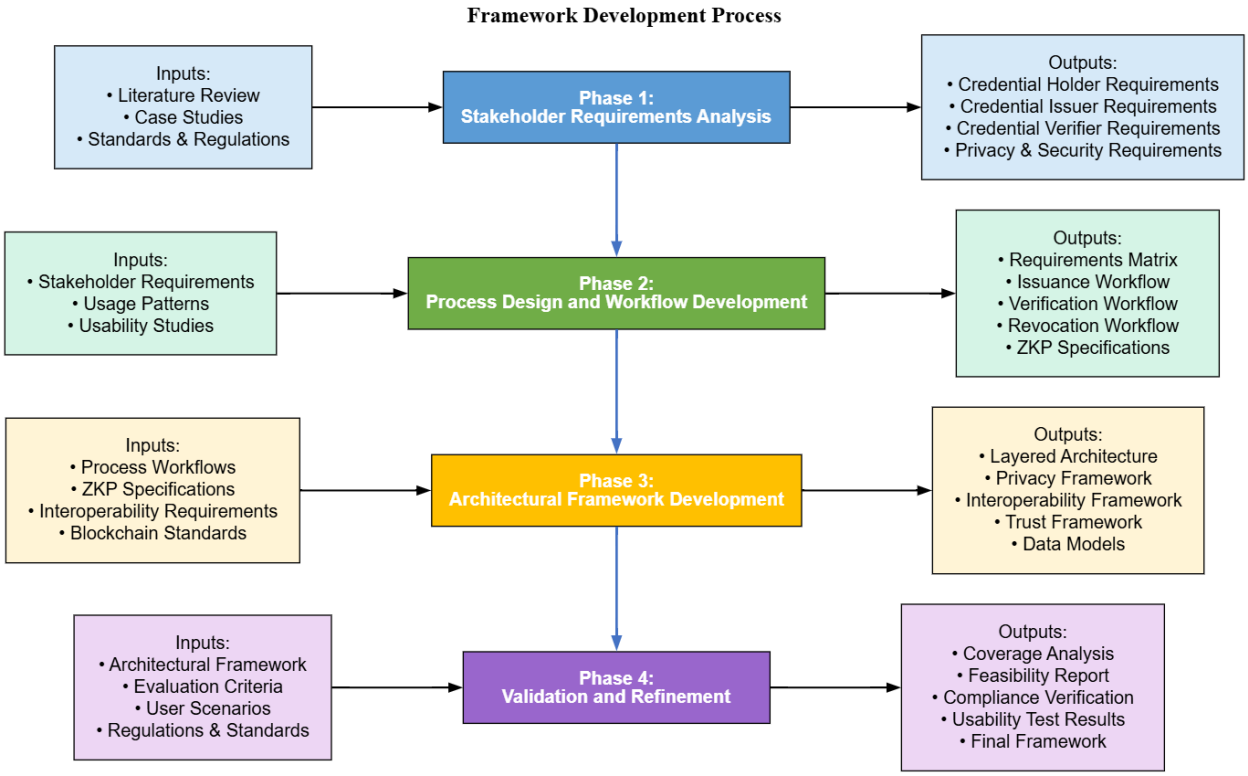


Fig 1: A Four-Phase Methodology for System Architecture Design

### 3.1 Phase 1: Problem Analysis and Requirements Engineering

The foundational phase established comprehensive problem understanding through systematic requirements engineering. This multi-dimensional analysis encompassed:

- **State-of-the-Art and Standards Review:** We conducted an extensive review of academic literature, existing operational systems, and relevant technical standards (e.g., W3C Verifiable Credentials, GDPR, FERPA) to establish current best practices and technological baselines.
- **Synthesis of System Requirements:** To anchor our framework in documented real-world needs, we performed a comprehensive synthesis of system requirements from the high-


Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

stakes domain of academic credentialing. This process involved systematically analyzing peer-reviewed studies, case analyses of deployed systems, and reports from standards bodies. This synthesis methodology enabled the construction of an evidence-based requirements landscape.

The derived requirements were categorized into three primary domains:

- **Credential Lifecycle & Data Integrity:** The analysis consistently highlighted the need for robust cryptographic mechanisms to ensure data authenticity throughout the credential lifecycle. Functional requirements for issuers include efficient, standardized issuance and fraud prevention, while verifiers require rapid, reliable, and cryptographically secure verification of both content and provenance.

- **Privacy & User-Controlled Disclosure:** The synthesis revealed a clear need for user-centric models. Core non-functional requirements for users include data ownership and control, operationalized through Self-Sovereign Identity (SSI) principles [20]. This is primarily realized through technical capabilities for **selective disclosure** via ZKPs and explicit, cryptographically signed consent mechanisms [44].

- **System Architecture & Non-Functional Requirements:** Architectural viability demands the satisfaction of critical non-functional requirements. The analysis identified **scalability**, **performance**, and **standards-based interoperability** as prerequisites for adoption [15], [45]. Seamless integration with existing enterprise systems (e.g., SIS, LMS) is also a key requirement to lower adoption barriers.

This synthesis revealed fundamental tensions between the demand for robust verification and the imperative for privacy and user control, confirming the necessity for a framework that formally reconciles these competing requirements through the synergistic integration of blockchain and ZKPs.

### 3.2 Phase 2: Formal Process and Workflow Modeling

This phase translated the synthesized requirements into formal operational workflows. Employing Business Process Model and Notation (BPMN), a standard for process modeling, and guided by PbD principles, we designed the core processes for credential issuance, verification, and revocation. A systematic analysis of these requirements yielded four guiding architectural principles:

- **Privacy-Preserving Verification by Default:** Mandate minimal data disclosure with cryptographic guarantees.

- **Interoperability Through Standardization:** Adhere to open, standards-based protocols for cross-platform functionality.

- **Integration-Ready Design:** Architect for seamless integration with existing enterprise information systems.

- **Granular Selective Disclosure:** Provide users with fine-grained, cryptographic control over information sharing.



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

These principles informed the workflow models, ensuring that privacy and security mechanisms were integral and foundational components of the system's logic.

### 3.3 Phase 3: Architectural Framework Construction

Based on these principles and formal workflows, we developed the layered architectural framework presented in this paper. This modular architecture, the central "design artifact" of this research, strategically integrates blockchain for establishing a trust anchor and ZKPs for privacy-preserving verification, while aligning with standards like W3C DIDs and VCs. The complete architecture is detailed in Section 4.

### 3.4 Phase 4: Theoretical Validation and Refinement

As the initial evaluation cycle, the framework underwent a rigorous theoretical validation, which is the focus of this paper. This involved: 1) a Requirement Coverage Analysis to formally assess how the architecture addresses the identified functional and non-functional requirements; 2) a Comparative Analysis benchmarking our design against existing solutions; and 3) a Technical and Regulatory Feasibility Assessment. The insights from this validation informed the final framework design and identified priorities for future empirical work.

## 4 The Proposed Framework

The architectural framework presented herein represents a paradigm shift from technology-first approaches to a holistic, modular system architected for secure, privacy-preserving, and pragmatic credential verification. Derived from our comprehensive requirements engineering process (Section 3), the framework operationalizes four foundational architectural principles:

- **Privacy-Preserving Verification by Default:** Leveraging Zero-Knowledge Proofs to enable claim validation without extraneous data disclosure.
- **Portability and Interoperability:** Facilitating seamless credential recognition across institutional and geographical boundaries through adherence to open standards.
- **Seamless Integration:** Prioritizing compatibility with existing enterprise information systems to minimize adoption friction.
- **User-Controlled Disclosure:** Providing users with granular, cryptographic control over their digital identity through self-sovereign mechanisms.

The framework employs a **stratified, four-layer architecture** (Figure 2), a common design pattern in systems engineering that ensures modularity, maintainability, and scalability.



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

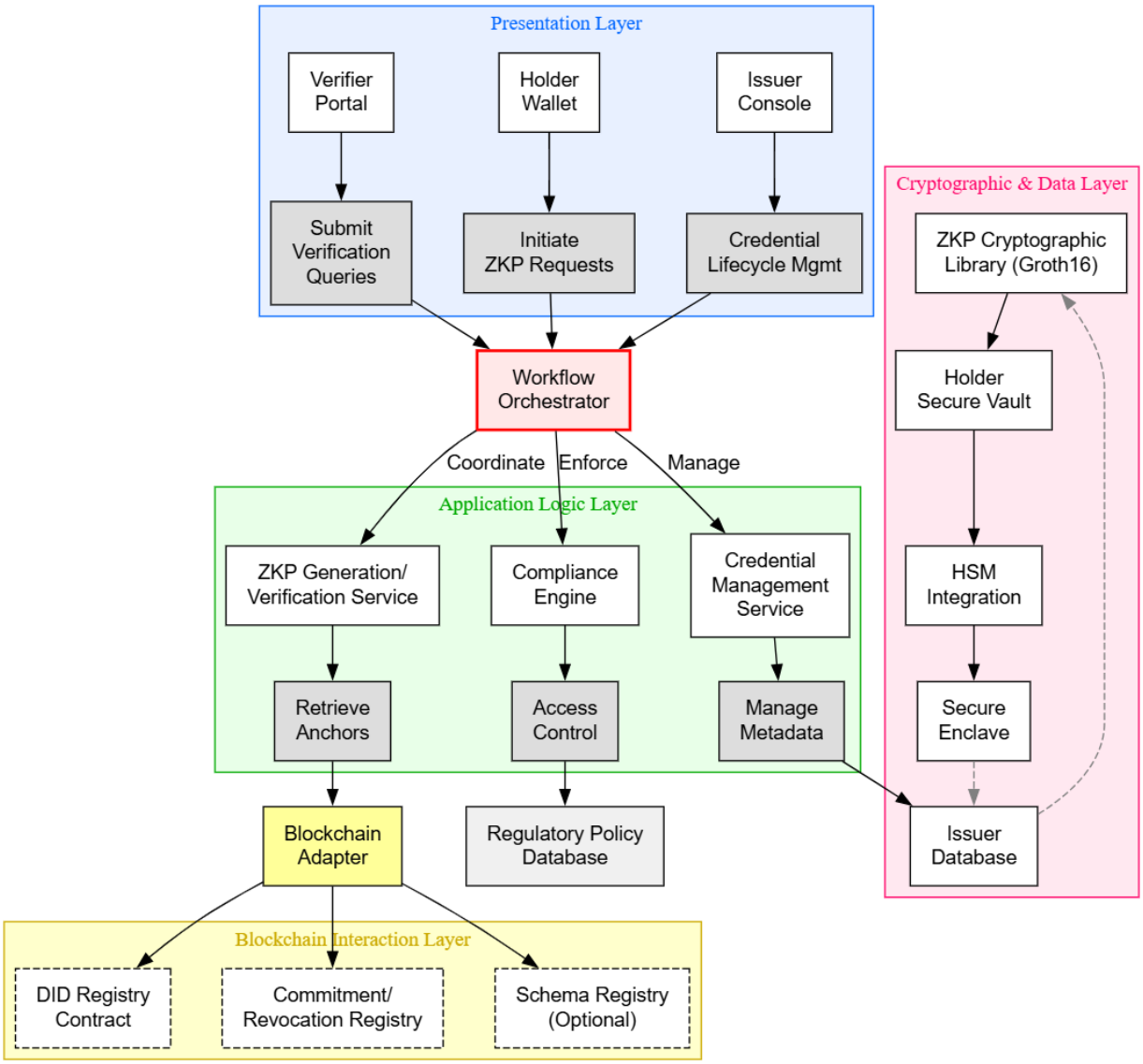


Fig 2: The Four-Layer System Architecture

Table 3 systematically maps the architectural components to the identified system requirements, demonstrating comprehensive coverage.

Table 3: Architectural Specification and Requirements Mapping

| Layer | Components | Key Functions | Technical & Stakeholder Requirements Addressed |
|---|---|---|---|
| Presentation | Holder Wallet, Issuer Console/API, Verifier Portal/API | User interaction interfaces, request initiation & consent management, result display, secure credential input/output. | Holder: Privacy, Ownership/Control, Accessibility. Issuer: Operational efficiency. Verifier: Efficient verification. Technical: |

Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

| Layer | Components | Key Functions | Technical & Stakeholder Requirements Addressed |
|---|---|---|---|
| | | | Usability, API integration. |
| Application Logic | Workflow Orchestrator, ZKP Service, Credential Management Service, Compliance Engine/IAM | Business process execution (issuance, verification, revocation), ZKP orchestration & policy enforcement, schema/metadata handling, identity & access management, audit logging. | Holder: Granular control. Issuer: Credential management, Regulatory compliance, Audit trails. Verifier: Streamlined/reliable verification. Technical: Performance logic, Scalability, Role-based access, Auditability. |
| Cryptographic & Data | ZKP Cryptographic Library, Holder Vault/Secure Storage, Issuer Data Store, KMS | Core ZKP generation/verification, secure storage of private keys & sensitive data, issuer record keeping, cryptographic key lifecycle management. | Holder: Security, Privacy. Issuer: Credential integrity, Secure storage. Verifier: Data accuracy. Technical: Crypto efficiency, Security protocols, Secure storage, Key management. |
| Blockchain Interaction | Blockchain Adapter, DID Registry, Commitment & Revocation Registry, Schema Registry | Abstraction of ledger communication, DID management (creation, resolution, revocation), anchoring commitments, managing credential revocation status, schema registration/retrieval. | Issuer: Integrity anchor, Revocation capability. Verifier: Verifiability, Trust anchor, Data minimization (via commitments). Technical: Interoperability, Blockchain considerations (consensus, cost, finality), Adherence to standards (DIDs). |

### 4.1 Architectural Layers and Components

The framework's stratified architecture embodies the principle of separation of concerns, ensuring robustness, maintainability, and evolutionary capability. Each component is designed



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

to address specific functional or non-functional requirements while maintaining system-wide coherence.

#### 4.1.1 Presentation Layer: The User Interface Gateway

The presentation layer mediates all human-system interactions through interfaces designed for usability, accessibility, and security:

- **Holder Wallet:** Transcending mere storage, this component serves as a comprehensive digital portfolio empowering users with self-sovereign credential management. It implements explicit, cryptographically-signed consent mechanisms for ZKP-based disclosures, directly operationalizing the principle of user agency.
- **Issuer Console/API:** A secure administrative interface enabling issuing authorities to orchestrate the complete credential lifecycle—from schema definition through issuance to revocation. The component is designed for seamless integration with enterprise systems (e.g., Student Information Systems), ensuring operational efficiency while maintaining data integrity.
- **Verifier Portal/API:** A streamlined interface architected for efficiency and trust, enabling verifiers to request and receive cryptographic validations while integrating seamlessly with existing recruitment or admission workflows.

#### 4.1.2 Application Logic Layer: The System's Core Engine

This layer constitutes the system's operational nucleus, orchestrating business logic and policy enforcement through four synergistic components:

- **Workflow Orchestrator:** The system’s central state machine, managing the credential lifecycle processes formalized in Section 4.2. It maintains operational state, coordinates inter-service communications, implements business rules, and ensures exception handling—guaranteeing reliable interactions throughout all operational workflows.
- **Zero-Knowledge Proof Service:** The core privacy engine enabling selective disclosure. Interfacing with the Holder Vault and the ZKP Cryptographic Library, it manages disclosure policies, optimizes the selection of cryptographic schemes, and ensures the integrity of the proof generation and verification process, all while enforcing strict consent protocols.
- **Credential Management Service:** Oversees credential schemas conforming to W3C Verifiable Credential standards, metadata management, and lifecycle orchestration. It bridges secure off-chain data stores with their on-chain trust anchors, supporting heterogeneous credential types while ensuring cross-platform interoperability.
- **Compliance Engine and IAM:** The framework’s governance and security guardian. It implements sophisticated access controls (Identity and Access Management - IAM) and is designed to be configurable for adherence to data protection frameworks (e.g., GDPR). This component establishes trust through demonstrable regulatory compliance and manages fine-grained permissions for all actors.



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

#### 4.1.3 Cryptographic & Data Layer: Trust and Privacy Foundation

This layer provides the core cryptographic operations and secure data storage mechanisms that underpin the entire framework.

- **ZKP Cryptographic Library:** The core engine responsible for all ZKP-related mathematics. It implements selected cryptographic schemes (e.g., zk-SNARKs, zk-STARKs), chosen based on a trade-off analysis of performance, proof size, and security assumptions. The integrity and correctness of this audited library are paramount to the system's security guarantees.
- **Secure Storage (Holder Vault, Issuer Data Store):** Provides secure, encrypted, off-chain storage for all sensitive data, including full credential details and private cryptographic keys. This architectural choice is fundamental to ensuring data sovereignty and confidentiality.

#### 4.1.4 Blockchain Interaction Layer

This layer abstracts all communication with the underlying distributed ledger, managing the immutable trust anchors for the system.

- **Blockchain Adapter:** A polymorphic interface designed to support multiple blockchain networks (e.g., Ethereum, Hyperledger Fabric, Polygon) through standardized abstractions. It encapsulates blockchain-specific protocols for transaction formatting and submission, ledger querying, and network communication, thereby enhancing modularity and platform adaptability.
- **DID Registry:** A smart contract that manages W3C-compliant Decentralized Identifiers, linking each DID to a DID Document containing public keys and service endpoints. This component establishes the cryptographic foundation for authenticating all actors and verifying data provenance.
- **Commitment & Revocation Registry:** A smart contract that serves two critical functions: (1) storing immutable cryptographic commitments (e.g., Merkle roots) of issued credentials, which are used for public ZKP verification, and (2) maintaining a transparent and append-only log of credential revocation statuses. This design elegantly balances the need for privacy (no PII on-chain) with the need for public verifiability and trust.
- **Schema Registry:** A hybrid on-chain/off-chain registry for managing credential schemas. It allows authorized issuers to register schemas publicly (often by placing a hash of the schema on-chain with a pointer to an off-chain location like IPFS), ensuring semantic interoperability and correct credential interpretation across the ecosystem.

### 4.2 Operational Workflows: The Framework in Action

This section delineates the framework’s core operational processes, demonstrating how the architectural components orchestrate to deliver privacy-preserving and user-centric credential management. The workflows presented in Figures 3-5 translate the system requirements into formal, executable protocols.



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

#### 4.2.1 Credential Issuance: Creating a Trustworthy and Private Digital Asset

The issuance workflow (Figure 3) exemplifies the framework's core architectural paradigm: **"off-chain data, on-chain trust anchor."** The process initiates with an authorized issuer preparing a credential according to a registered schema. Rather than exposing sensitive data on-chain, the system generates a **cryptographic commitment** (e.g., a Merkle root or Pedersen commitment) to the credential data. This commitment, alongside the issuer's DID and a pointer to the revocation registry, is immutably recorded in an on-chain smart contract. The complete credential, containing all private attributes, is then transmitted through a secure, off-chain channel to the holder's wallet. This architectural decision is fundamental to preserving user privacy while establishing a public, cryptographic guarantee of the credential's existence and integrity.

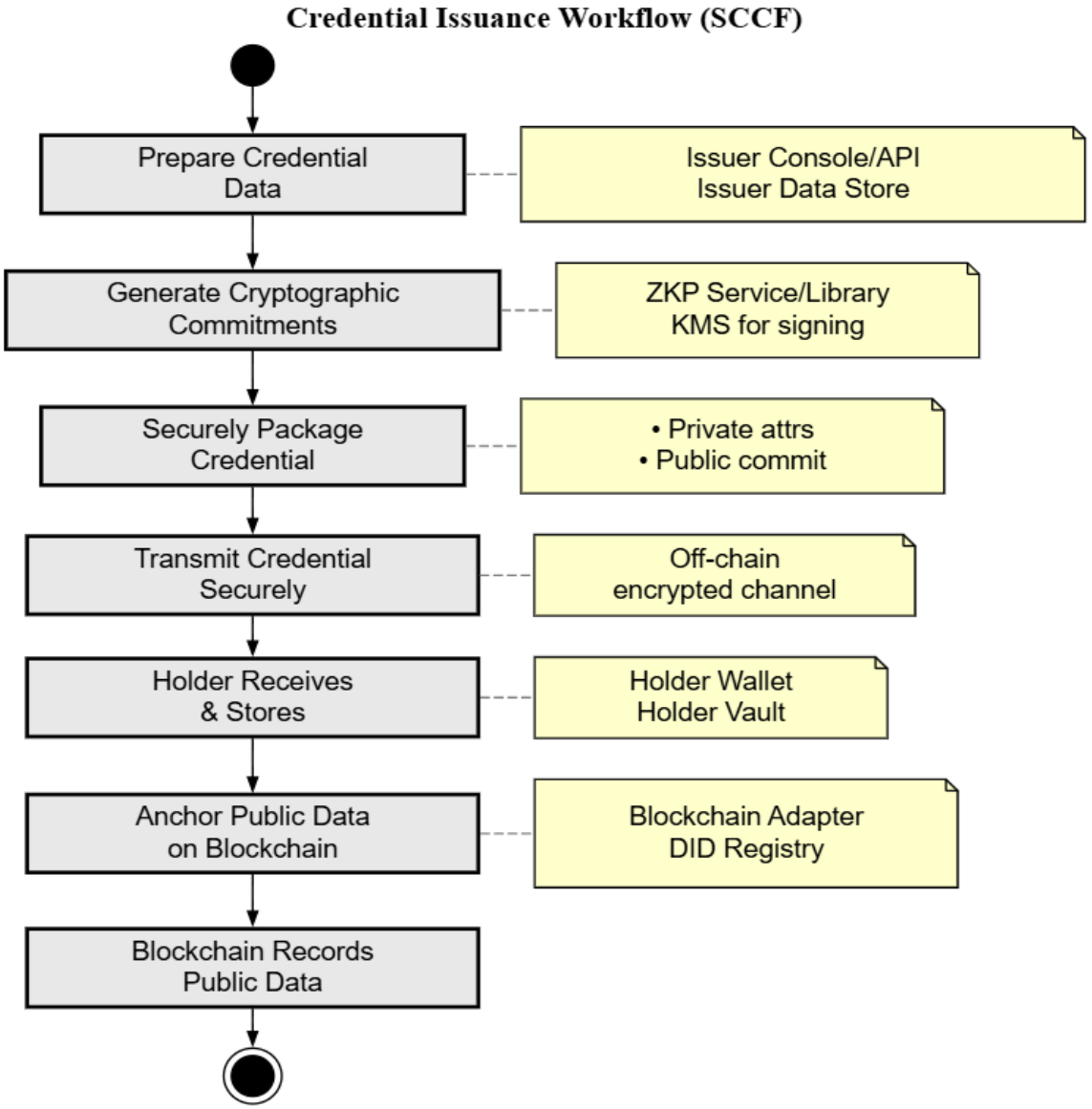


Figure 3: Credential Issuance Workflow



Received: August 13 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

### 4.2.2 Credential Verification

The verification workflow (Figure 4) represents the framework's most innovative contribution, enabling trustworthy verification while enforcing user data sovereignty. The process unfolds as a ZKP-mediated, three-party protocol involving the verifier, the holder, and the blockchain infrastructure.

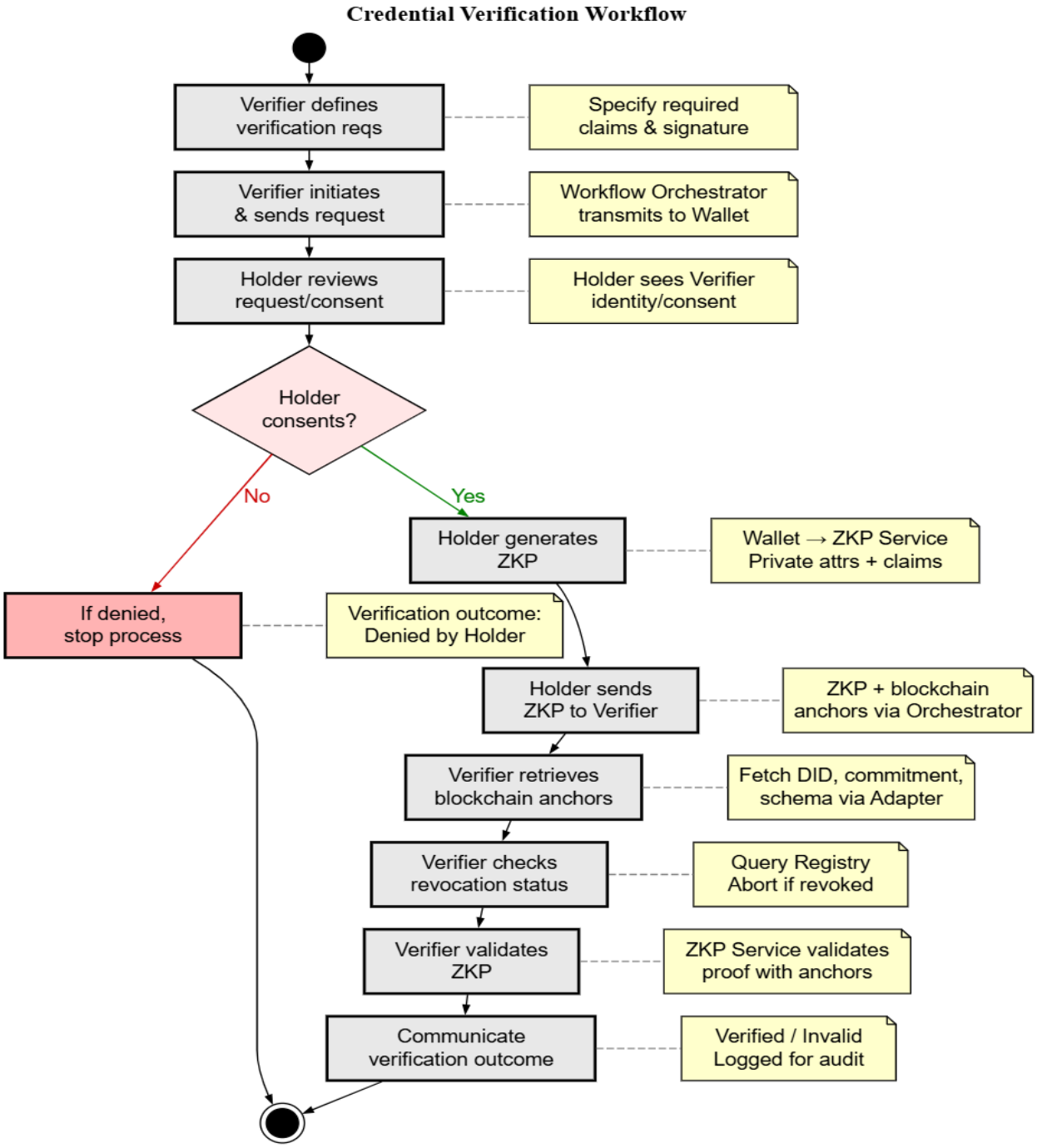


Figure 4: Credential Verification Workflow

Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Verification initiates when a verifier submits a digitally signed request specifying the precise claims requiring validation (the "statement" to be proven). This request is routed to the holder's wallet, triggering a critical, user-driven consent decision. The holder must review the request and provide explicit, cryptographically-signed consent before the protocol can proceed. This step is a direct implementation of the user empowerment requirement.

Upon consent, the holder's device (or a designated service) generates a **Zero-Knowledge Proof**. This proof cryptographically demonstrates that the holder's private credential data satisfies the verifier's requested claims, without revealing any of the underlying data itself. The generated proof is transmitted to the verifier, who then validates it against the publicly available information anchored on the blockchain (the issuer's public key via their DID, the cryptographic commitment, and the credential's current revocation status). A successful validation provides the verifier with strong cryptographic assurance of the claim's validity while preserving the holder's privacy—achieving the seemingly paradoxical goal of verification without disclosure.

### 4.2.3 Credential Revocation: Maintaining Ecosystem Integrity

The revocation workflow (Figure 5) ensures the continued trustworthiness of the ecosystem by enabling the transparent and authoritative invalidation of credentials under legitimate circumstances (e.g., administrative errors or policy violations). An authorized issuer submits a cryptographically signed transaction to the on-chain revocation registry, which is immutably linked to the original credential commitment. The smart contract authenticates the transaction using the issuer’s private key, preventing unauthorized revocations while ensuring the immediate and public propagation of any status change. Since the verification protocol (Section 4.2.2) mandates a check against this on-chain registry, any attempt to verify a revoked credential will fail instantly, thus maintaining the integrity of the entire ecosystem.

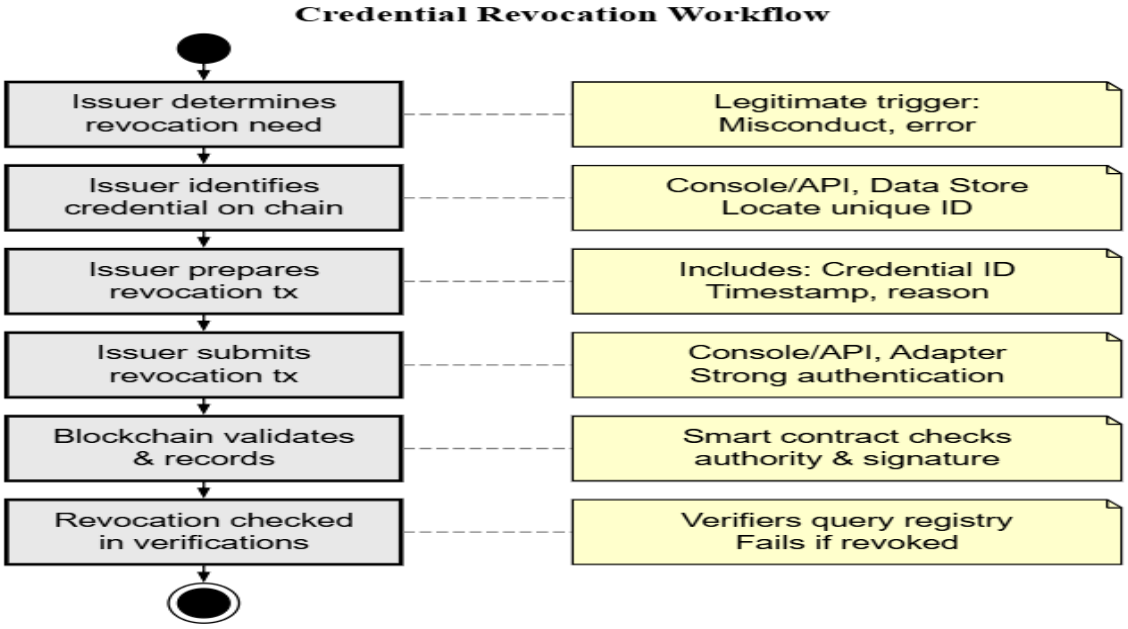


Fig 5: Credential Revocation Workflow



Received: August 13 2025

International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

## 5 Architectural Analysis

This section presents a theoretical analysis of the proposed architectural framework. Instead of qualitative requirements check, we evaluate the design's soundness by analyzing its core technical properties from a systems engineering and applied cryptography perspective. The analysis is structured around the principal design goals of any secure distributed system: security, privacy, performance, and interoperability.

### 5.1 Security Analysis: Integrity and Authenticity

The framework's security model is built upon cryptographic primitives that provide strong guarantees of data integrity and authenticity.

- **Data Integrity:** The integrity of issued credentials is mathematically enforced by anchoring a **cryptographic commitment** (e.g., a Merkle root) on an immutable distributed ledger. Any attempt to tamper with the off-chain credential data would invalidate its correspondence to the on-chain commitment, making forgery computationally infeasible to conceal. The **soundness property** of the underlying ZKP scheme further ensures that a holder cannot generate a valid proof for a false or altered statement.

- **Authenticity and Provenance:** The use of W3C Decentralized Identifiers (DIDs) provides a robust mechanism for authentication. Each entity (issuer, holder, verifier) is associated with a DID linked to a set of public keys. All critical actions, such as issuing or revoking a credential, must be signed by the issuer's private key. This allows any party to cryptographically verify the provenance of a credential and the authenticity of its status, preventing unauthorized actions.

- **Revocation and Liveness:** The on-chain revocation registry provides a transparent and censorship-resistant mechanism for maintaining the real-time validity of credentials. As the verification protocol mandates a check against this registry, the system is protected against the use of credentials that are no longer valid.

### 5.2 Privacy Analysis: Data Minimization by Design

Privacy in this architecture is not an add-on feature but a **cryptographically enforced property** derived directly from the principles of data minimization and the mathematical guarantees of ZKPs.

- **Zero-Knowledge Property:** The core of the privacy model is the **zero-knowledge property** of the ZKP protocol. This mathematically guarantees that the verifier learns nothing beyond the validity of the specific statement being proven. This allows the system to achieve verification without disclosure, fundamentally protecting user data.

- **Off-Chain Data Storage:** A critical architectural choice is the strict separation of private data from the public ledger. All personally identifiable information (PII) is stored exclusively in secure, off-chain repositories (the Holder Vault and Issuer Data Store) under the control of the respective parties. Only non-private, abstract data (commitments, DIDs,



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

revocation status) is anchored on-chain. This "off-chain data, on-chain trust anchor" paradigm is central to the framework's privacy model.

- **User Consent as a Protocol Step:** Data sovereignty is enforced at the protocol level. The verification workflow mandates an explicit, cryptographically signed consent from the holder before any ZKP generation can occur. This transforms privacy from a policy statement into a non-bypassable step in the system's operational logic.

### 5.3 Performance and Scalability Considerations

The architecture is designed to mitigate the performance and scalability bottlenecks commonly associated with blockchain and ZKP technologies.

- **ZKP Computation:** The most computationally intensive task is the generation of a ZKP by the holder's device. The performance of this task is directly coupled to the **mathematical complexity of the arithmetic circuit** representing the assertion being proven. By design, all ZKP computations occur entirely off-chain, placing no load on the blockchain itself. The modular ZKP Cryptographic Library is designed to incorporate optimized circuits for common assertions and to support efficient, modern ZKP schemes (e.g., those based on PLONK or Halo2) that do not require a per-circuit trusted setup.

- **Blockchain Throughput and Cost:** The framework is designed to minimize on-chain interactions. Instead of placing each credential on the ledger, only a single, small cryptographic commitment is recorded. Furthermore, these commitments can be batched; for example, the Merkle root of thousands of credentials can be anchored in a single on-chain transaction, drastically reducing the cost and data footprint per credential. The Blockchain Adapter also provides the flexibility to deploy the system on high-throughput, low-cost Layer 2 solutions or permissioned ledgers, bypassing the scalability limitations of public Layer 1 blockchains.

### 5.4 Comparative Analysis and Novelty

The novelty of this framework lies not in the individual technologies it employs, but in its holistic architectural design that synergistically integrates them to resolve a fundamental paradox in digital verification.

- **Resolution of the Integrity-Privacy Paradox:** While first-generation blockchain systems (e.g., Blockcerts) provided data integrity, they did so at the cost of privacy by requiring "all-or-nothing" data disclosure for verification. Our framework resolves this tension. The blockchain layer provides the public trust anchor for integrity, while the cryptographic layer (ZKP) provides mathematically verifiable privacy.

- **From Protocol to System Architecture:** While other research has explored ZKPs for credentials, many studies focus narrowly on the cryptographic protocol itself. The primary contribution of this work is a comprehensive, end-to-end **system architecture** that provides a practical blueprint for translating the theoretical guarantees of ZKPs into a robust, scalable, and interoperable information system. It addresses the entire lifecycle of a credential and considers



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the practical requirements of a multi-party ecosystem, thus bridging the gap between cryptographic theory and systems engineering.

## 6 Conclusion

The secure verification of digital credentials in distributed systems presents a fundamental tension between the need for public verifiability and the imperative of user privacy. While blockchain technology provides a robust foundation for data integrity, its inherent transparency can compromise the confidentiality of sensitive information. This research addressed this challenge by proposing a formal, layered architecture that synergistically integrates the integrity guarantees of blockchain with the privacy-preserving properties of Zero-Knowledge Proofs (ZKPs).

Distinctly, our approach was not technology-first; it was founded on a rigorous requirements engineering process that informed the design of a modular architectural blueprint. This requirements-driven methodology led to the development of privacy-by-design operational protocols for credential issuance, verification, and revocation, where complex cryptographic primitives are applied to solve practical system-level problems.

The framework's principal contribution is its four-layer modular architecture, which provides a concrete design pattern for translating the mathematical guarantees of ZKPs into a functional, large-scale system. A key architectural principle is the judicious use of the blockchain as a decentralized trust anchor, not as a data repository. All sensitive data remains off-chain under the user's control, while only non-private cryptographic elements—such as Decentralized Identifiers (DIDs), cryptographic commitments, and revocation statuses—are anchored on-chain to ensure transparency, auditability, and integrity. Our architectural analysis confirms that this design resolves the integrity-privacy paradox inherent in earlier systems, advancing security and operational efficiency beyond both traditional mechanisms and first-generation blockchain-based solutions.

In conclusion, this research presents a comprehensive, requirements-driven architecture that significantly advances privacy and user control in digital credential verification. By adhering to open standards (W3C VCs/DIDs) and embedding privacy-preserving cryptographic protocols at its core, the proposed framework offers a practical and theoretically sound blueprint for the next generation of trustworthy digital credentialing infrastructure.

## 7 Future Work

While this paper establishes a robust theoretical foundation and a formal architectural blueprint, transitioning from conceptual design to a production-grade system requires significant further research. Future work should proceed along three key technical tracks:

- **Empirical Performance Analysis and Optimization:** The immediate priority is the development of a prototype to conduct empirical validation of the system's performance. This includes benchmarking ZKP generation and verification times on various client devices for common assertion types, measuring on-chain transaction costs under different batching strategies, and analyzing end-to-end system latency under simulated load.



Received: August 13 2025

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **Advanced Cryptographic Integration and Formal Security Analysis:** Future research should investigate the integration of more advanced ZKP schemes, such as zk-STARKs or recursive ZKPs, to eliminate trusted setups and enhance scalability. A crucial next step is to conduct a **formal security analysis** of the proposed protocols, creating security proofs under established cryptographic models (e.g., the Universal Composability framework) to formally verify the privacy and integrity guarantees of the system.
- **Decentralized Governance and Interoperability Protocols:** The long-term success of such a framework depends on robust governance and interoperability. Future work should focus on designing and modeling **decentralized governance mechanisms** (e.g., through DAOs) for managing shared components like the DID and Schema registries. Furthermore, research is needed to develop and standardize cross-ledger interoperability protocols to ensure that credentials verified through this framework can be seamlessly recognized across different blockchain ecosystems.

References

[1] T. Chandra, M. Kaur, N. Rakesh, M. Gulhane, and S. Maurya, "Novel blockchain-based framework to publish, verify, and store digital academic credentials of universities," *International Journal of Information Technology*, vol. 16, no. 5, pp. 3273–3281, 2024. https://doi.org/10.1007/s41870-024-01842-w

[2] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024. https://doi.org/10.1016/j.jisa.2023.103678

[3] A. S. Alammary, "Building a Sustainable Digital Infrastructure for Higher Education: A Blockchain-Based Solution for Cross-Institutional Enrollment," *Sustainability*, vol. 17, no. 1, p. 194, 2025. https://doi.org/10.3390/su17010194

[4] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, and F. Wendland, "Blockchain for education: lifelong learning passport," in *Proceedings of the 1st ERCIM Blockchain Workshop 2018*, 2018. https://doi.org/10.18420/blockchain2018_07

[5] G. Caldarelli and J. Ellul, "Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review," *Applied Sciences*, vol. 11, no. 4, p. 1842, 2021. https://doi.org/10.3390/app11041842

[6] 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.2022.3206791

[7] A. Choudhary, M. Chawla, and N. Tiwari, "Analyzing functional, technical and bibliometric trends of blockchain applications in education: A systematic review," *Multimedia Tools and Applications*, pp. 1–46, 2024. https://doi.org/10.1007/s11042-024-20303-x



Received: August 13 2025

**Volume 38 No. 7s, 2025**

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8] E. Tan, E. Lerouge, J. Du Caju, and D. Du Seuil, "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 79, 2023. https://doi.org/10.3390/bdcc7020079

[9] S. M. Vaezinejad, C. Ying, M. Kouhizadeh, and K. Ozpolat, "Blockchain Technology for Higher Education and Recruitment: A Systematic Literature Review," *Eurasian Journal of Business and Economics*, vol. 17, no. 33, pp. 1–27, 2024. https://doi.org/10.17015/ejbe.2024.033.01

[10] F. Loukil, M. Abed, and K. Boukadi, "Blockchain adoption in education: a systematic literature review," *Education and Information Technologies*, vol. 26, no. 5, pp. 5779–5797, 2021. https://doi.org/10.1007/s10639-021-10481-8

[11] R. Poorni, M. Lakshmanan, and S. Bhuvaneswari, "DIGICERT: a secured digital certificate application using blockchain through smart contracts," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, 2019, pp. 215–219. https://doi.org/10.1109/ICCES45898.2019.9002576

[12] G. Capece, N. Levialdi Ghiron, and F. Pasquale, "Blockchain technology: Redefining trust for digital certificates," *Sustainability*, vol. 12, no. 21, p. 8952, 2020. https://doi.org/10.3390/su12218952

[13] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, 2020. https://doi.org/10.1016/j.jnca.2020.102731

[14] X. Wang, M. Younas, Y. Jiang, M. Imran, and N. Almusharraf, "Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges," *IEEE Access*, vol. 13, pp. 13264-13284, 2025. https://doi.org/10.1109/ACCESS.2024.3519350

[15] Y. Kistaubayev, G. Mutanov, M. Mansurova, Z. Saxenbayeva, and Y. Shakan, "Ethereum-based information system for digital higher education registry and verification of student achievement documents," *Future Internet*, vol. 15, no. 1, p. 3, 2022. https://doi.org/10.3390/fi15010003

[16] D. L. Fekete and A. Kiss, "Toward building smart contract-based higher education systems using zero-knowledge Ethereum virtual machine," *Electronics*, vol. 12, no. 3, p. 664, 2023. https://doi.org/10.3390/electronics12030664

[17] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "SNARKs for C: Verifying program executions succinctly and in zero knowledge," in *Advances in Cryptology – CRYPTO 2013*, 2013, pp. 90–108. https://doi.org/10.1007/978-3-642-40084-1_6



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[18] D. Benarroch, M. Campanelli, D. Fiore, K. Gurkan, and D. Kolonelos, "Zero-knowledge proofs for set membership: Efficient, succinct, modular," *Designs, Codes and Cryptography*, vol. 91, no. 11, pp. 3457–3525, 2023. https://doi.org/10.1007/s10623-023-01245-1

[19] S. Tyagi and S. Tyagi, "A Review on Zero Knowledge Proof Vulnerabilities in Zcash," in *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, 2023, pp. 872–877. https://doi.org/10.1109/ICAICCIT60255.2023.10466054

[20] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," *Sensors*, vol. 25, no. 11, p. 3450, 2025. https://doi.org/10.3390/s25113450

[21] A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, and M. Y. Shams, "Unlocking the power of blockchain in education: An overview of innovations and outcomes," *Blockchain: Research and Applications*, vol. 4, no. 4, p. 100165, 2023. https://doi.org/10.1016/j.bcra.2023.100165

[22] Z. Li, K. L. Joseph, J. Yu, and D. Gasevic, "Blockchain-based Solutions for Education Credentialing System: Comparison and Implications for Future Development," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 79–86. https://doi.org/10.1109/Blockchain55522.2022.00021

[23] M.-F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday*, vol. 25, no. 9, 2020. https://doi.org/10.5210/fm.v25i9.10654

[24] S. I. M. Ali, H. Farouk, and H. Sharaf, "A blockchain-based models for student information systems," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 187–196, 2022. https://doi.org/10.1016/j.eij.2021.12.002

[25] M.-C. Nguyen-Ngoc et al., "ZUni: The Application of Blockchain Technology in Validating and Securing Educational Credentials," in *Intelligence of Things. ICIT 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol. 188, 2023, pp. 258–268. https://doi.org/10.1007/978-3-031-46749-3_25

[26] Y. Qingyi, W. Liangmin, P. Senshan, Z. Yifan, and L. Jiayi, "AssessChain: A hybrid blockchain-based system for transparent and reliable online assessment," *Education and Information Technologies*, vol. 29, no. 15, pp. 20665–20689, 2024. https://doi.org/10.1007/s10639-024-12713-z

[27] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers & Security*, vol. 99, p. 102050, 2020. https://doi.org/10.1016/j.cose.2020.102050

[28] B. Bünz, A. Chiesa, W. Lin, P. Mishra, and N. Spooner, "Proof-Carrying Data Without Succinct Arguments," in *Advances in Cryptology – CRYPTO 2021*, 2021, pp. 681–710. https://doi.org/10.1007/978-3-030-84242-0_24



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[29] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, 2019, pp. 203–225. https://doi.org/10.1145/3335741.3335752

[30] X. Xu, "Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities," *Smart Learning Environments*, vol. 11, no. 1, p. 7, 2024. https://doi.org/10.1186/s40561-024-00294-w

[31] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, 2016. [Online]. Available: https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/

[32] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash Protocol Specification," 2016. [Online]. Available: https://github.com/zcash/zips/blob/master/protocol/protocol.pdf

[33] D. Shadung, S. Mthethwa, S. Ntshangase, T. Singano, and N. Mokoena, "Self-sovereign Identity Management System Using Verifiable Credentials to Enhance Privacy and Security Through Zero Knowledge Proofs," in *The 5th Joint International Conference on AI, Big Data and Blockchain (ABB 2024). Lecture Notes in Networks and Systems*, vol. 881, 2024, pp. 15–34. https://doi.org/10.1007/978-3-031-73151-8_2

[34] T.-D. Tran et al., "CrossCert: A Privacy-Preserving Cross-Chain System for Educational Credential Verification Using Zero-Knowledge Proof," in *Industrial Networks and Intelligent Systems. INISCOM 2024. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 595, 2024, pp. 256–271. https://doi.org/10.1007/978-3-031-67357-3_18

[35] V.-T. Doan and T.-D. Trinh, "Zero-Knowledge-Proof-Based Protocol Connecting Traditional Finance to Decentralized Finance," in *The International Conference on Intelligent Systems & Networks (ICISN 2024)*, 2024, pp. 406–415. https://doi.org/10.1007/978-981-97-5504-2_48

[36] R. Joshi, S. K. Gupta, R. Natarajan, K. Pandey, and S. Kumari, "Blockchain-Powered Monitoring of Healthcare Credentials through Blockchain-Based Technology," in *Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions*, 2025, pp. 170–199. https://doi.org/10.2174/9789815305210125010011

[37] M. Lupu and I. Aciobăniței, "Enhanced Blockchain-Based e-Voting System Using Zero-Knowledge Proofs," in *Proceedings of the International Conference on Informatics in Economy (IE 2024)*, 2024, pp. 237–246. https://doi.org/10.1007/978-981-96-0161-5_21



Received: August 13 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[38] P. Ohlhaver, M. Nikulin, and P. Berman, "Compressed to 0: The Silent Strings of Proof of Personhood," *Stanford Journal of Blockchain Law & Policy*, vol. 8, p. 60, 2025. https://dx.doi.org/10.2139/ssrn.4749892

[39] A. Hardy, "Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance," *Internet Policy Review*, vol. 13, no. 3, pp. 1–31, 2024. https://doi.org/10.14763/2024.3.1785

[40] D. Ramiro Troitiño and V. Mazur, "e-Identity: A Step Forward to European Digital Citizenship," in *E-governance in the European Union: Strategies, Tools, and Implementation*, 2024, pp. 57–70. https://doi.org/10.1007/978-3-031-56045-3_5

[41] S. Barab and K. Squire, "Design-Based Research: Putting a Stake in the Ground," *The Journal of the Learning Sciences*, vol. 13, no. 1, pp. 1–14, 2004. https://doi.org/10.1207/s15327809jls1301_1

[42] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, Canada, 2009.

[43] B. L. Parmar, R. E. Freeman, J. S. Harrison, A. C. Wicks, L. Purnell, and S. De Colle, "Stakeholder theory: The state of the art," *The Academy of Management Annals*, vol. 4, no. 1, pp. 403–445, 2010. https://doi.org/10.5465/19416520.2010.495581

[44] Š. B. Ramić, E. Cogo, I. Prazina, M. Turkanović, R. T. Mulahasanović, and S. Mrdović, "Selective disclosure in digital credentials: A review," *ICT Express*, 2024. https://doi.org/10.1016/j.icte.2024.05.011

[45] M. Gottlieb, C. Deutsch, F. Hoops, H. Pongratz, and H. Krcmar, "Expedition to the blockchain application potential for higher education institutions," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100203, 2024. https://doi.org/10.1016/j.bcra.2024.100203



Received: August 13 2025