Design and Analysis of a Self-Sovereign Identity (SSI) Platform for Fraud-Free Academic Verification: A Review

Project Guide: **Prof. Abhay Gaidhani**
[abhay.gaidhani@sitrc.org] Department of Computer Engineering
Sandip Institute of Technology and Research Centre

Ved Prakash Jadhav
Department of Computer Engineering
Sandip Institute of Technology and Research Centre
Nashik, Maharashtra, India
vedj889@gmail.com

Namit Pramod Gahane
Department of Computer Engineering
Sandip Institute of Technology and Research Centre
Nashik, Maharashtra, India
namitgahane@gmail.com

Aditya Vilas Navghare
Department of Computer Engineering
Sandip Institute of Technology and Research Centre
Nashik, Maharashtra, India
navghareaditya4@gmail.com

Bhushan Valmik Ghuge
Department of Computer Engineering
Sandip Institute of Technology and Research Centre
Nashik, Maharashtra, India
bhushan12ghuge@gmail.com

Abstract—Academic credentials underpin hiring, admissions, and professional licensing decisions, yet the manual, paper-based, and centralized systems used to issue and verify them remain slow and forgeable. Diploma mills and altered transcripts continue to circulate at scale, and existing digital-verification services still route trust through a single central authority. This paper presents a comprehensive review of blockchain- and Self-Sovereign Identity (SSI)-based academic credentialing published between 2016 and 2026 and, based on the synthesized literature, formulates an SSI platform built on the W3C Decentralized Identifier (DID) and Verifiable Credential (VC) standards. Institutions act as issuers that sign VCs bound to a graduate's DID; students hold and control these credentials in a personal digital wallet; and employers or other institutions act as verifiers that check the credential's signature and revocation status against a permissioned blockchain trust registry, without contacting the issuing institution directly. Zero-knowledge selective disclosure lets a holder reveal only the attributes a verifier needs, reducing over-disclosure of personal data, while a rule-based fraud-pattern layer flags diploma-mill and altered-transcript indicators. Component boundaries, the credential lifecycle, Merkle-accumulator revocation, and evaluation metrics—verification latency, fraud-detection precision and recall, disclosure minimization, and on-chain cost—are systematically detailed without reporting uncollected empirical data.

Index Terms—Self-sovereign identity, decentralized identifiers, verifiable credentials, blockchain, academic credential fraud, zero-knowledge proofs, selective disclosure, trust registry, credential revocation.

I. Introduction

Degrees, diplomas, and transcripts issued by academic institutions are the evidentiary basis for hiring, further admissions, and professional licensing. That evidentiary role has made credentials a persistent fraud target. The single largest documented diploma-mill operation, Axact, ran thousands of fictitious institution websites and sold fraudulent credentials to more than eight million buyers across 191 countries before its 2015 takedown [1]. Industry estimates place the fake-degree market at roughly seven billion dollars a year in direct sales alone, with additional indirect costs borne by employers and institutions that must investigate and re-verify suspect documents [2]. Traditional mitigations—calling the registrar, mailing sealed transcripts, or paying a third-party verification service—are slow, costly, and still route trust through a single central authority that can be compromised, be slow to respond, or simply cease to exist [3].

Self-Sovereign Identity (SSI) reframes this problem around the credential holder rather than a central directory. Under SSI, an individual generates and controls cryptographic identifiers and stores signed credentials in a personal digital wallet, presenting only what a given interaction requires [4], [5]. Two W3C standards make this practical at scale: Decentralized Identifiers (DIDs), a URI-based identifier scheme that lets an entity prove control of an identifier without a centralized registry [6]; and the Verifiable Credentials (VC) Data Model, a standard, cryptographically verifiable format for expressing claims made by an issuer about a subject [7]. Together, DIDs and VCs let an academic institution issue a tamper-evident digital

credential that a graduate can carry and present anywhere, and that any verifier can cryptographically check without contacting the institution.

To address these challenges, this paper proposes an SSI-based platform for fraud-free academic verification that combines DID/VC issuance by institutions, custody by students, and blockchain-anchored verification by employers or other institutions, together with zero-knowledge selective disclosure so that only the minimum necessary attributes are revealed in any single verification.

The primary contributions of this review paper are organized as follows:

- A structured review of academic-credential fraud, blockchain-anchored credentialing, standards-based SSI, and privacy-preserving disclosure and revocation, summarized in a comparison table.
- A multi-role system architecture that separates credential custody (holder wallet) from institutional trust anchoring (permissioned registry), keeping personal data off-ledger by design.
- A detailed methodology integrating W3C DID/VC issuance, zero-knowledge selective disclosure, Merkle-accumulator revocation, and a rule-based fraud-pattern layer.
- A mathematical and evaluation framework defining the verification decision rule, revocation proof length, latency, fraud-detection precision and recall, and disclosure-minimization metrics.

II. Literature Survey and Review Method

The literature published between 2016 and 2026 was surveyed across four core domains: academic-credential fraud and conventional verification; blockchain-anchored credential systems; standards-based SSI built on DIDs and VCs; and privacy-preserving disclosure and revocation. This review prioritizes peer-reviewed articles, open standards, and recent preprints, and Table I summarizes representative works.

A. Academic Credential Fraud and Conventional Verification

Diploma mills and altered transcripts are the two dominant forgery patterns documented in the literature [3], [2]. Conventional verification—direct registrar contact, sealed paper transcripts, or commercial clearinghouses—is manual and slow, and depends on a central party remaining available and uncompromised [1].

B. Blockchain-Anchored Credential Systems

Early schemes anchor credential hashes on a public ledger. Blockcerts batches credentials into a Merkle root written to Bitcoin [8], and BTCert adds a multi-signature issuing committee [9]. These schemes prove that a credential existed and was unmodified since issuance, but they disclose the whole document and offer no fine-grained revocation or selective disclosure. Permissioned-ledger systems such as CredenceLedger add institutional control over who may write to the registry but predate the DID/VC standards [10]. Lightweight anchoring on low-power nodes has also been benchmarked for throughput and energy [11]. A 2026 security analysis of the deployed Block.co platform further shows that anchoring a credential to a blockchain does not by itself guarantee unforgeability [12].

C. Standards-Based SSI and DID/VC Platforms

Sovrin and Hyperledger Indy provide a public-permissioned ledger with RBFT consensus and AnonCreds zero-knowledge credentials [13], [14]. A recent comparative study identifies Indy, Sovrin, and LifeID as the strongest candidates for academic credential management [15], and education-specific work on Indy demonstrates schema interoperability with the European Diploma Supplement and ECTS frameworks [16]. VCTP extends issuer trust beyond institutions to individuals [17].

D. Privacy-Preserving Disclosure and Revocation

Zero-knowledge selective disclosure allows a holder to prove a predicate over credential attributes without revealing the credential itself [13], [14]. Recent surveys and preprints on blockchain-based privacy applications and SSI-based academic credential management confirm that consent, minimal disclosure, and revocation are the recurring open design issues [18], [19]. Reading Table I across rows shows a clear split: anchoring schemes prove existence but leak the whole document, while standards-based SSI platforms add selective disclosure but have rarely been evaluated against academic-fraud patterns.

TABLE I
REPRESENTATIVE WORKS ON BLOCKCHAIN- AND SSI-BASED ACADEMIC CREDENTIALING, 2016–2026

Work (year)	Method / Approach	Contribution	Limitation
Blockcerts (2016) [8]	Bitcoin Merkle-root batch anchoring	First open standard for blockchain-anchored credentials	No selective disclosure or revocation privacy
BTCert (n.d.) [9]	Merkle-root + multisig issuing committee	Third-party verification without a central authority	High transaction fees; coarse batch revocation
CredenceLedger (2018) [10]	Permissioned blockchain ledger	Institution-controlled trust anchor	No DID/VC standardisation; no privacy layer

Work (year)	Method / Approach	Contribution	Limitation
Sovrin / Hyperledger Indy [13], [14]	Public-permissioned ledger, RBFT, AnonCreds ZKP	Zero-knowledge selective disclosure of attributes	Requires steward governance; adoption overhead
Indy education architecture (2026) [16]	DID + VC + revocation registry over Indy	Schema interoperability across EU Diploma Supplement / ECTS	Evaluated only against European frameworks
Energy-efficiency evaluation (2025) [11]	Lightweight anchoring on low-power nodes	Practical throughput / energy benchmarking	No privacy-preserving disclosure mechanism
Comparative study of SSI models (2026) [15]	Compares EverID, LifeID, Sora, SelfKey, Indy, Sovrin	Identifies Indy/Sovrin/LifeID as strongest for education	Comparative only; no working implementation
Block.co forgery analysis (2026) [12]	Security analysis of a deployed platform	Demonstrates a real forgery vulnerability in production	Anchoring alone does not guarantee unforgeability
VCTP (2023) [17]	Trust-propagation protocol for personal issuers	Extends issuer trust to individuals	Not evaluated for high-volume institutional issuance

III. Research Gap and Problem Definition

Taken together, the literature has not converged on a single system that combines standards-compliant DID/VC issuance, blockchain-anchored institutional trust, zero-knowledge selective disclosure, and a revocation mechanism, evaluated specifically against academic-credential fraud patterns such as diploma-mill forgeries and altered transcripts. Anchoring-only systems disclose the whole document, standards-based platforms have been assessed mainly on interoperability, and a deployed system has already been shown to be forgeable despite blockchain anchoring [12].

The objective of this research is to formulate a standards-compliant, privacy-preserving verification platform in which trust is rooted in cryptography and a permissioned registry rather than in a call to the issuing institution. To ensure deterministic verification, a presentation p of credential c issued by institution I is accepted if and only if all four checks pass:

$$A(p) = V_{sig}(\sigma, pk_I) \wedge V_{did}(DID_I) \wedge V_{rev}(c) \wedge V_{zk}(\pi, P) \quad (1)$$

where V_{sig} verifies the issuer's signature σ against public key pk_I, V_{did} confirms that the issuer DID resolves to an accredited institution on the registry, V_{rev} confirms that c is not revoked, and V_{zk} verifies the zero-knowledge proof π for the requested predicate P. Fraud-pattern flags are advisory and do not enter A(p), which keeps a human decision in the loop.

IV. Proposed System Architecture

The proposed platform follows the standard SSI trust triangle of issuer, holder, and verifier, anchored to a permissioned blockchain that stores only DID documents and revocation status—never the credential content itself, which stays with the holder. It is structured into five modular layers. Fig. 1 illustrates the roles, the registry, and the information exchanged between them.

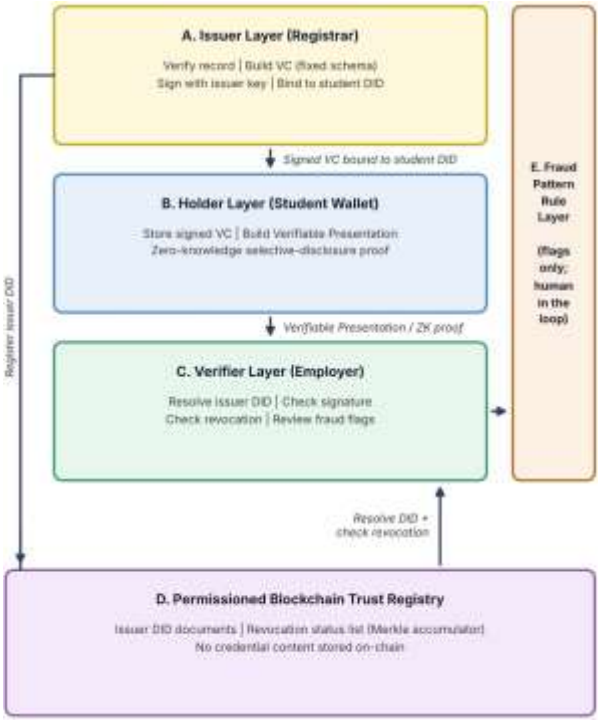


Fig. 1. SSI platform architecture: issuer–holder–verifier layers anchored to a permissioned blockchain trust registry.

A. Issuer Layer and Credential Issuance

The institution's registrar system acts as issuer. After confirming a student's academic record internally, it constructs a Verifiable Credential using a fixed schema (degree, division, CGPA band, date of conferral, institution DID) and signs it with the institution's private key, binding the credential to the student's DID as the credentialSubject.

B. Holder Layer: Custody and Presentation

The student stores the signed VC in a personal wallet application. When a verifier requests proof of a qualification, the wallet constructs a Verifiable Presentation. Rather than sending the full VC, the wallet can generate a zero-knowledge selective-disclosure proof that reveals only the requested predicate—for instance, that a CGPA exceeds a threshold or that a specific degree was conferred—without exposing the full transcript, following the AnonCreds-style proof approach used in Hyperledger Indy [13], [14].

C. Permissioned Blockchain Trust Registry

The institution's DID document—containing its public verification key—is registered once on the permissioned ledger, together with a revocation status list. Individual student credentials are never written to the chain, keeping personal data off-ledger by design. The registry therefore acts only as a shared, tamper-evident source of issuer keys and revocation state.

D. Verifier Layer

The verifier resolves the issuer's DID from the registry, checks the credential signature against the issuer's published public key, and checks the revocation status list anchored on-chain. A lightweight rule layer additionally surfaces fraud-pattern flags, described in Section V-C, to the verifier.

V. Detailed Methodology and Algorithm Formulation

A. Credential Lifecycle Sequence

System implementation and validation follow a structured phased methodology. First, the institution registers its DID document on the permissioned ledger and fixes the credential schema. Second, the registrar verifies the student's record and issues a signed VC to the student's DID. Third, the student stores the VC in the wallet. Fourth, on a verifier's request the wallet builds a zero-knowledge selective-disclosure proof. Fifth, the verifier checks the signature and resolves the issuer DID. Sixth, the revocation status is checked. Finally, the verifier receives any fraud-pattern flags and makes an accept or reject decision. Fig. 2 summarizes the full pipeline.

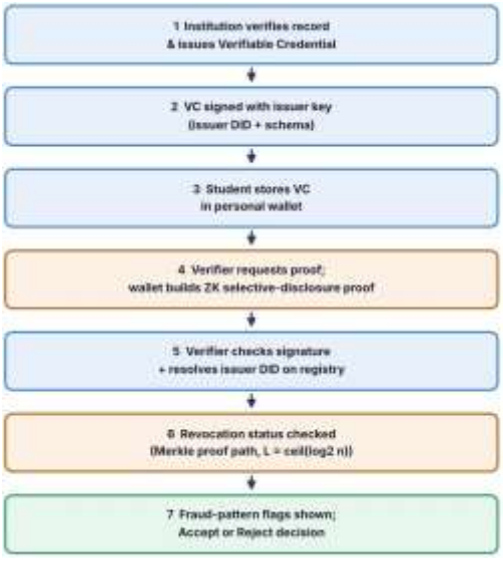


Fig. 2. End-to-end credential issuance and verification pipeline.

B. Revocation and Constant-to-Logarithmic Verification Cost

Because revocation status is a small bitstring or Merkle-accumulator entry rather than the credential itself, a check is a constant-to-logarithmic-time lookup rather than a call back to the institution. For a registry holding n active revocation entries organized as a Merkle accumulator, a revocation check requires retrieving a proof path of length

$$L = \lceil \log_2 n \rceil \tag{2}$$

hashes, so verification cost grows logarithmically rather than linearly with registry size, which keeps per-check latency low as the number of issued credentials grows.

C. Fraud-Pattern Detection

Independently of cryptographic verification, a lightweight rule layer flags presentation patterns associated with known fraud types documented in the literature: credentials whose issuer DID does not resolve to an accredited institution, duplicate serial or credential identifiers across unrelated holders, and issuance dates inconsistent with an institution's operating history—patterns characteristic of diploma-mill and altered-transcript fraud [3], [2]. Flags are surfaced to the verifier rather than silently blocking a presentation, keeping a human decision in the loop.

VI. Evaluation Framework and Metrics

Because the system is at design stage, no synthetic or uncollected performance numbers are claimed; instead, the evaluation framework fixes the protocol and metrics that a follow-up implementation study will report against. Four categories of measurement are planned.

A. Verification Performance

End-to-end latency is measured from presentation request to accept/reject decision, $T_v = t_{decision} - t_{request}$, together with throughput in verifications per second under concurrent load, benchmarked against a traditional call-the-registrar baseline.

B. Fraud-Detection Effectiveness

Precision and recall of the rule layer are measured against a labelled set of genuine credentials mixed with synthetic diploma-mill-style forgeries, altered-transcript variants, and replayed or expired credentials, per the standard definitions

$$P = TP/(TP + FP), \quad R = TP/(TP + FN) \tag{3}$$

where TP, FP, and FN are true positives, false positives, and false negatives over the labelled evaluation set.

C. Privacy and Disclosure Minimization

The number of attributes disclosed per verification event is compared with the number requested and with disclosing a full transcript. For a credential with $|A_t|$ attributes of which $|A_d|$ are disclosed, the disclosure ratio is

$$\rho = |A_d| / |A_t| \quad (4)$$

where the ideal value equals the fraction of attributes the verifier actually requested.

D. Cost and Scalability

On-chain storage and transaction cost are recorded per issued institution DID and per revocation update, and verification latency is measured as the number of registered institutions and active credentials grows, following the low-power-node benchmarking approach used in prior blockchain-credential work [11].

VII. Expected Outcomes, Benefits, and Limitations

The expected outcome of this research is a fully specified, evaluation-ready SSI platform for academic verification. By letting verifiers check signatures and revocation status against the registry, the design removes the need to contact the issuing institution, makes forged or altered credentials cryptographically detectable, and limits personal-data exposure through selective disclosure.

Several practical limitations must be acknowledged. Standards-based networks such as Sovrin require steward governance and carry adoption overhead [13]. Institutions must be onboarded and accredited before their DIDs are trusted, and students must safeguard wallet keys. Anchoring alone does not guarantee unforgeability, so the proof and revocation design must be implemented carefully [12]. Finally, the rule layer may produce false positives, and the evaluation relies on synthetic forgeries until real issuance data are available.

VIII. Future Scope

Future extensions include implementing the platform on Hyperledger Indy and measuring the metrics defined in Section VI; aligning credential schemas with the European Diploma Supplement and ECTS frameworks [16]; deploying lightweight verification on low-power nodes [11]; extending trust to peer-issued credentials such as micro-credentials and certifications [17]; and adding wallet key-recovery mechanisms and offline verification for low-connectivity settings.

IX. Conclusion

This review surveyed blockchain- and SSI-based academic credentialing work from 2016 to 2026 and found no published system that combines standards-compliant DID/VC issuance, blockchain-anchored institutional trust, zero-knowledge selective disclosure, and revocation, evaluated specifically against academic-credential fraud. We proposed a platform that fills that gap: institutions issue W3C-standard Verifiable Credentials bound to student DIDs, students hold and selectively disclose them from a personal wallet, and verifiers check signatures and revocation status against a permissioned blockchain registry without contacting the institution directly. A rule-based layer flags presentation patterns associated with known diploma-mill and transcript-alteration fraud. The evaluation framework sets up the measurements a follow-up implementation study will report.

References

[1] VerifyED, "Diploma Mill List 2026: How to Check If a School Is Fake," VerifyED Guides, 2026. [Online]. Available: https://verifyed.org/guides/diploma-mill-list-2026

[2] Parchment, "Diploma Mills and Academic Fraud: The Hidden Global Financial Impact," Parchment Blog, 2025. [Online]. Available: https://www.parchment.com/blog/global-financial-impact-of-diploma-mills-and-academic-fraud/

[3] A. Ezell and J. Bear, "Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas," Amherst, NY, USA: Prometheus Books, 2012.

[4] A. J. Zwitter, O. J. Gstrein, and E. Yap, "Digital identity and the blockchain: Universal identity management and the concept of the 'self-sovereign' individual," Front. Blockchain, vol. 3, art. 26, 2020.

[5] Sovrin Foundation, "Self-Sovereign Identity: A Comprehensive Guide to Decentralized Identity Management," Sovrin Foundation Rep., 2020. [Online]. Available: https://sovrin.org

[6] World Wide Web Consortium, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022. [Online]. Available: https://www.w3.org/TR/did/

[7] World Wide Web Consortium, "Verifiable Credentials Data Model v2.0," W3C, 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[8] P. Schmidt, "Blockcerts: An open infrastructure for academic credentials on the blockchain," 2016. [Online]. Available: https://www.blockcerts.org

[9] BlockTechCert, "BTCert: Academic certificate authentication via Blockcerts," GitHub repository, accessed 2026. [Online]. Available: https://github.com/BlockTechCert/BTCert

[10] R. Arenas and P. Fernandez, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," in Proc. IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC), 2018, pp. 1–6.

[11] "Design, implementation and practical energy-efficiency evaluation of a blockchain-based academic credential verification system for low-power nodes," arXiv:2410.20605, 2025.

[12] "A forgery attack on the Block.co blockchain-based digital credential certification system," arXiv:2606.31462, 2026.

[13] D. Reed, J. Law, and D. Hardman, "The Technical Foundations of Sovrin," Sovrin Foundation, White Paper, 2016.

[14] "A survey of self-sovereign identity ecosystem," arXiv:2111.02003.

[15] W. Samara, A. Alyammahi, and S. Sangheethaa, "A comparative study of self-sovereign identity models for managing academic credentials," in Proc. Springer Conf. Ser., 2026, doi: 10.1007/978-981-96-4136-9_37.

[16] "Governance and interoperability of verifiable educational credentials: An information systems architecture based on Hyperledger Indy," Comput., Mater. Continua, 2026.

[17] "VCTP: A verifiable credential-based trust propagation protocol for personal issuers in self-sovereign identity platforms," arXiv:2308.01539, 2023.

[18] "A survey of blockchain-based privacy applications: An analysis of consent management and self-sovereign identity approaches," arXiv:2411.16404, 2024.

[19] "Secure academic credential management using blockchain-based self-sovereign identity," preprint, ResearchGate, 2025.