Privacy Preserving Academic Credential Verification Using Permissioned Blockchain

Srijib Samanta
Assistant Professor and Head of Department (HOD), Department of Bachelor of Computer Application (BCA) Tamralipta Institute of Management & Technology

***Abstract*—Academic credential verification must establish confidence in an issuer's claims without exposing unnecessary student information. Blockchain can support shared governance, but does not independently establish academic truth, confidentiality or current credential validity. This conceptual paper proposes a permissioned architecture in which holders retain signed credentials while a consortium maintains issuer authorization, key history and commitments to versioned status information. A focused review of primary research and technical standards informs the trust model, disclosure rules, lifecycle procedures and evaluation protocol. Verification distinguishes proof validity, issuer acceptance, holder binding, claim conditions and status freshness. The proposed experiments compare a conventional signed-credential service, a permissioned registry, purpose-specific credentials and an optional selective-disclosure variant under matched policies. Outcomes cover incorrect acceptance and rejection, disclosure, presentation correlation, revocation propagation, verification latency, throughput and operating cost. The analysis identifies why a valid signature need not establish academic correctness, why recorded revocation need not imply fresh verification, and why proof-level unlikability need not prevent identification through visible attributes. No prototype results or measured gains are claimed. The contribution is an assessment framework for testing whether shared ledger custody adds sufficient assurance to justify its cost and complexity.**

***Index Terms*—Academic credentials; permissioned blockchain; verifiable credentials; privacy; revocation; selective disclosure.**

I. INTRODUCTION

Graduates present qualifications to universities, employers and professional bodies, often years after leaving the issuer. A verifier needs reliable evidence of the award and its current acceptability. A student should also be able to establish a narrow qualification without routinely sharing an entire transcript. Authenticity, institutional trust and minimum disclosure are therefore connected requirements.

A valid signature can accompany a mistaken grade or an improperly approved award. A blockchain can preserve the related event without correcting the administrative decision. MIT's digital-diploma pilot and EduCTX already demonstrate educational blockchain applications (Durant & Trachy, 2017; Turkanović et al., 2018). The present contribution is a controlled evaluation of assurance, disclosure and status freshness rather than a claim that blockchain-based credentials are new.

1.1 Research problem and objectives

The problem is to verify academic claims while rejecting altered, untrusted, expired or revoked evidence and avoiding unnecessary disclosure. Permissioned membership restricts participation but still exposes some metadata to authorized operators. Frequent credential-specific status queries can also reveal when and where a graduate seeks verification.

The objectives are to define the evidence and trust requirements; design a registry that minimizes student data; specify revocation, correction and key-management procedures; and construct separate security, privacy and performance assessments. No operational deployment at Tamralipta Institute of Management & Technology is asserted.

1.2 Research questions

Question	Proposition to be tested
RQ1 What does a permissioned ledger add to signed credentials?	P1 Recording cannot establish academic correctness, but may improve shared custody of governance history.
RQ2 What disclosure and correlation risks remain?	P2 Minimization reduces exposure while stable attributes and status metadata can still link presentations.
RQ3 How do publication and caching affect revocation?	P3 Freshness policies reduce stale acceptance but may increase inconclusive decisions during outages.
RQ4 What costs arise under load and failures?	P4 Consensus and replication add costs whose value depends on demonstrable operational assurance.

1.3 Methodological approach

The paper uses a focused, purposive synthesis of primary publications, standards and official documentation. It develops requirements, an architecture and a proposed evaluation protocol rather than a systematic review or completed experiment. Planned tests use fictitious academic records. Successful synthetic verification would establish protocol behavior, not the legitimacy of real qualifications. An authorized institutional pilot would require separate evidence about registrar procedures and user experience.

II. RELATED RESEARCH AND STANDARDS

2.1 Educational systems and the evaluation gap

Durant and Trachy (2017) describe MIT's holder-shared digital-diploma pilot. Turkanović et al. (2018) examine higher-education credits through EduCTX. Gupta (2024) studies permissioned credential verification using Hyperledger Fabric, while Berrios Moya et al. (2025) propose zero-knowledge-enabled academic-record verification. These studies establish relevant precedents; their reported outcomes cannot be transferred to an unimplemented architecture. The evaluation gap addressed here is the separation of cryptographic validity, institutional trust and current status, with a strong non-blockchain comparator. A fast valid-signature result is incomplete when fresh revocation evidence is missing. Equally, revealing fewer fields can still permit identification through a persistent student number. A combined success score can conceal both failures.

2.2 Credential and presentation specifications

The W3C Verifiable Credentials Data Model v2.0 supplies an issuer–holder–verifier model, while Verifiable Credential Data Integrity 1.0 addresses authenticity and integrity evidence (World Wide Web Consortium [W3C], 2025b, 2025c). Both cited editions became Recommendations on 15 May 2025. OpenID for Verifiable Presentations 1.0 supplies a presentation protocol (OpenID Foundation, 2025). Deployment still requires compatible schemas, proof formats and acceptance policies.

Bitstring Status List v1.0 supports aggregate status publication and discusses tracking risks (W3C, 2025a). The proposed design uses signed list versions and explicit freshness checks. Aggregate publication reduces particular query risks but does not remove correlation through stable list references or disclosed identity.

The pinned Data Integrity BBS Crypto suites v1.0 edition is a Candidate Recommendation Draft dated 10 September 2026 (W3C, 2026). It is an optional research extension, not a final Recommendation. Supported derived proofs can selectively disclose claims; proving an undisclosed numerical threshold requires an appropriate additional mechanism or a separately signed eligibility claim.

2.3 Infrastructure and key management

Hyperledger Fabric supplies permissioned membership and configurable ordering (Androulaki et al., 2018). Raft crash tolerance and BFT malicious-node tolerance require different tests (Hyperledger Fabric, n.d.). Key protection and lifecycle controls remain essential (Barker, 2020): ordinary rotation, issuer-key compromise and holder-key loss have different consequences for historical verification and recovery.

III. REQUIREMENTS TRUST BOUNDARIES AND THREATS

The framework requires intact credential evidence, authorized issuance, appropriate holder binding,

satisfied claim conditions, current acceptable status and minimum necessary disclosure. Issuer enrolment records the institution's permitted assertions and relevant key periods. Verifiers define which issuers, credential types and evidence ages they accept. Registry membership alone does not make every claim acceptable for every purpose.

The academic source system is a distinct trust boundary. Course completion, grades and award approval depend on institutional processes. Record reconciliation, approval controls and correction procedures address that boundary. Consensus cannot independently validate a student's educational history. Cryptographic assurance must therefore be reported separately from confidence in the underlying administrative decision.

Table 1 Threats and the corresponding assessment

Threat	Control or policy	Evaluation boundary
Altered or fabricated credential	Proof validation and issuer trust checks	A trusted issuer can still sign inaccurate content.
Stolen file or replayed presentation	Supported holder binding and fresh request context	The selected profile must actually implement these checks.
Unauthorized status modification	Publisher authorization and signed list commitments	Authorization does not establish the fairness of revocation.
Stale or unavailable status	Evidence-age limits and explicit inconclusive outcome	An unavailable list does not prove revocation.
Curious verifier or operator	Minimal claims and restricted records	Visible identity and timing can still support correlation.
Compromised keys or operators	Key-lifecycle controls and declared fault model	Protection is bounded by implementation and governance assumptions.

Primary tests assume correctly implemented cryptography, protected private keys, authenticated registry evidence and a verifier clock within a stated tolerance. Stress tests relax selected assumptions. Full compromise of every governance authority, coerced disclosure outside the protocol and academically false claims approved by trusted issuers are not solved by the ledger. Potential observers are assessed separately: a verifier sees disclosed attributes; a status service sees fetch activity; a ledger operator sees registry events. Combining these views is a stronger collusion scenario and must be declared. Security and privacy claims identify the observer, exposed information and applicable fault assumptions.

IV. PROPOSED CREDENTIAL ARCHITECTURE

4.1 Roles and storage

An issuer creates and signs a credential after academic approval. A holder receives it through authenticated delivery and retains it in a wallet or protected repository. A verifier requests purpose-relevant evidence and applies the trust and status policy. The consortium governs issuer enrolment, key history and commitments to status-list versions. Its members need not receive each student's complete credential.

Names, student numbers, grades, transcript files and credential-specific verification logs are excluded from routine ledger replication. Protected issuer systems retain academic source records, and holders retain signed credentials. The ledger stores issuer authorizations, key events, profile references and status commitments. Content-addressed storage is not confidential merely because a file is identified by a hash.

4.2 Issuance and presentation

The credential profile fixes field names, data types, proof format, issuer identity, validity conditions and status reference. Canonicalization and verification follow the selected suite. Optional archival batch commitments require protected opening information; hashes of predictable names or grades neither encrypt the record nor establish its truth.

The verifier states the purpose and requested claims. A fresh challenge and verifier-specific context bind the exchange as supported by the selected protocol.

Narrow, separately signed assertions provide one minimization route. A selective-disclosure suite provides another. Removing fields from an ordinary signed document does not preserve its original signature, and partial claims cannot generally reproduce the original full-document hash.

Table 2 Evidence locations and normal access

Evidence	Location	Normal access
Academic source records	Protected institutional system	Authorized institutional staff
Complete signed credential	Holder wallet and protected backup	Holder and authorized recovery service
Requested presentation	Holder–verifier exchange	Intended verifier
Issuer and key history	Permissioned registry	Consortium and approved readers
Signed status lists	Retrievable status infrastructure	Verifiers under publication policy
List-version commitments	Permissioned ledger	Approved registry readers

4.3 Status verification and consortium governance

An authorized publisher signs each status-list version. The registry binds the list identifier and version to its digest and publication event. A verifier validates the signature, checks the retrieved bytes against the commitment and applies freshness rules. A correctly authenticated old list is still old evidence; a ledger reference does not automatically make it current.

Endorsement policy determines who may enroll issuers, change keys or publish status commitments. Ordering determines event sequence. Administrative ownership and key custody are recorded separately from node counts. Raft experiments concern crash faults; BFT experiments concern malicious operators within the chosen implementation's threshold (Hyperledger Fabric, n.d.). Four independently administered orders may support a one-fault BFT scenario where its assumptions hold.

Issuer retirement and consortium exit require continuity arrangements for key history, status archives and authenticated checkpoints. Preserving historical evidence does not require indefinite replication of private academic records. Historical signature validity and present acceptance remain separate decisions.

V. CREDENTIAL LIFECYCLE AND EVIDENCE FRESHNESS

5.1 Revocation suspension and correction

Revocation means that a credential should no longer be accepted under the relevant policy. Suspension is temporary where supported. Correction replaces erroneous claims and specifies the old credential's status. Expiration follows validity conditions. Revoking compromised digital evidence need not invalidate the underlying degree; reissuance may preserve a valid award (W3C, 2025a). Private disciplinary or correction reasons remain in authorized case records.

5.2 Publication caching and propagation

A change is authorized, reflected in a signed list, committed under the publication policy and made available to verifiers. Each step receives its own timestamp. Revocation propagation is measured from authorization to correctly rejecting decisions across verifier instances. Transaction acknowledgment is not substituted for confirmed commitment or refreshed status.

With enforced maximum publication delay p and refresh interval c, propagation can approach p + c, plus network and processing delay, under normal availability. This is a conditional engineering bound, not an unconditional security guarantee. Longer caching can reduce service requests and latency while extending stale-state exposure. Outages require explicit timeout and inconclusive-decision rules.

5.3 Rotation compromise and recovery

Routine issuer-key rotation retains approved historical verification information. Compromise requires identification of the affected period, review of uncertain credentials and reissuance where needed. A date inside a signature made with a stolen key cannot independently establish pre-compromise issuance. Witnessed records or trusted issuance commitments can strengthen temporal evidence;

otherwise, the uncertainty remains explicit (Barker, 2020).

Holder-key loss also requires authorized recovery. Re-establishing possession must not silently transfer the credential to an unauthorized person. Device failure, accessibility and offline use require an assisted route. Offline verification can assess available evidence but cannot claim knowledge of the latest revocation state.

5.4 Structured acceptance decisions

Acceptance requires every mandatory condition: supported proof validity; acceptable issuer and key; appropriate holder binding; satisfied claim and validity conditions; and sufficiently fresh acceptable status. A failed condition leads to rejection. Missing mandatory evidence leads to an inconclusive or unavailable outcome rather than silent acceptance.

Table 3 verification decisions

Scenario	Expected decision	Meaning
Trusted current evidence and all mandatory checks pass	Accept under policy	Does not independently establish academic truth.
Altered signed claim	Reject	Cryptographic evidence is invalid.
Fresh status confirms revocation	Reject	A valid signature cannot override current status.
Status too old or unreachable	Inconclusive or unavailable	Current acceptability cannot be established.
Issuer not authorised for the requested claim	Reject under policy	A contextual trust decision, not a universal judgment.
Required presenter binding fails	Reject or seek specified evidence	Depends on the actual supported binding method.

VI. PRIVACY ANALYSIS

Minimum disclosure is defined by purpose. Degree confirmation may not require semester marks, date of birth or unrelated awards. The evaluation records what the verifier actually receives. Holder approval improves transparency but cannot by itself prevent excessive requests when refusing would block an educational or employment opportunity. Request-policy review and an alternative verification route therefore remain necessary.

6.1 Privacy analysis continued

Randomized proof values do not hide a repeatedly disclosed name, stable wallet key or status index. The analysis distinguishes proof-level unlikability from whole-presentation correlation. Aggregate fetching, caching and independent distribution can reduce observable queries without eliminating all metadata. Small actual list populations and closely timed changes may weaken group privacy despite a large nominal list capacity.

The optional BBS extension tests supported selective disclosure and proof verification with a pinned implementation. It does not assume arbitrary predicates over hidden grades or universal wallet compatibility. A separately signed eligibility claim may meet a narrow purpose without disclosing the underlying mark. Disclosure counts are useful descriptions, not a complete measure of privacy.

VII. PROPOSED EVALUATION PROTOCOL

7.1 Comparator configurations

Table 4 Configurations isolating system contributions

Code	Credential model	Infrastructure and comparison
V0	Signed full-disclosure credentials	Conventional registry, signed lists and witnessed checkpoints; non-blockchain reference.
V1	Same profile and acceptance rules as V0	Permissioned registry with matched lists and retention; isolates ledger effects.
V2	Purpose-specific signed claims	Same registry as V1; examines disclosure minimization.

Code	Credential model	Infrastructure and comparison
V3	Supported selective-disclosure proofs	Matched registry and issuer semantics; examines proof-processing and disclosure trade-offs.

V0 is a strong conventional system rather than an unsecured database. V0 and V1 use identical credentials, status freshness, trust rules and workloads. V2 and V3 retain equivalent claim meaning and policy wherever technically feasible. Differences caused by proof format, holder binding or disclosure cannot be attributed to the ledger alone.

7.2 Synthetic workloads

Tests use 5, 10 and 20 simulated issuers with 10,000, 100,000 and 1,000,000 fictitious credentials. Profiles include degrees, course certificates, issue periods and controlled status changes. Credential population is distinguished from list capacity. The Bitstring Status List validation algorithm defaults to at least 131,072 entries unless an ecosystem specifies another lower bound (W3C, 2025a). These are planned workloads, not collected institutional data.

7.3 Security privacy and availability tests

Security scenarios include modified claims, invalid signatures, untrusted issuers, replayed contexts, missing holder binding, unauthorized status changes and concurrent verification during revocation. Valid cases accompany negative cases so that rejecting everything cannot appear successful. Scenarios with false but authentically issued claims expose unresolved academic-governance risk rather than a cryptographic failure.

Observers receive only their role-specific view. Presentation-linking tests use balanced same-holder and different-holder pairs and compare against appropriate chance baselines. Colluding observer views are a separate condition. Service loss, storage failure and ordering disruption are tested within declared fault assumptions. Warm-cache and cold-cache cases retain evidence-age information.

Table 5 Outcomes and interpretation requirements

Dimension	Measure	Interpretation
Decision security	Incorrect acceptance and rejection by scenario	Retain valid controls and inconclusive outcomes.
Disclosure and correlation	Unnecessary fields and presentation-linking success	Identify observer, visible metadata and baseline.
Revocation	Authorization-to-correct-rejection interval	Include publication, commitment and cache delays.
Verification performance	End-to-end p50, p95 and p99 latency and decisions per second	Separate cache states and count failures.
Infrastructure	CPU, memory, traffic, storage and operational effort	Record ownership, replication and retention.
Availability	Accepted, rejected and inconclusive request fractions under faults	Fast failure is not completed verification.

7.4 Analysis and reproducibility

At least five independent workload seeds are proposed per feasible condition, with repeated deployments where needed. A pilot sets the final replication plan. Paired traces support run-level differences and confidence intervals; requests within one deployment are not independent replications of the whole system. Tail quantiles require sufficiently long runs. Issuance, commitment, proof checking and final decisions receive separate timings and denominators.

The reproducibility package records synthetic generation, credential profiles, proof and dependency versions, key assumptions, seeds, clock tolerances, list sizes, cache rules, consensus, hardware and network conditions. Failed runs and raw timings are

retained. Evidence archives exclude live private keys and personal data.

VIII. CONCEPTUAL ANALYSIS AND DISCUSSION

The framework yields three central deductions. First, proof validity, issuer trust and academic correctness answer different questions. A registry can preserve evidence about who was authorized to issue a claim; institutional processes establish whether the award was justified. A permissioned ledger may strengthen shared custody where institutions do not accept a sole historian. Witnessed conventional records may meet the same need at lower cost.

Second, revocation freshness is an end-to-end property. A committed event provides little protection if a verifier accepts stale evidence without declaring its age. Conversely, an unreachable status service does not prove that a credential is revoked. Preserving inconclusive outcomes exposes the security cost of outages and prevents availability failures from being hidden inside favorable latency figures.

Third, privacy depends on the entire presentation. Minimizing ledger data limits replication but cannot undo information disclosed directly to a verifier. Selective proofs reduce supported disclosure while identity and status references may still link transactions. Publication schedules, caching and list population affect both privacy and operational performance. The appropriate trade-off depends on the credential purpose and approved policy.

Standards improve interoperability within compatible profiles; they do not remove schema, proof-format or wallet mismatches. The BBS draft remains work in progress in this proposal. Cross-implementation checks should distinguish baseline conformance from optional functionality. None of these deductions establishes a measured throughput, privacy gain or deployment-readiness claim.

9 Ethics limitations and future research

Initial tests use fictitious records and isolated infrastructure. A real pilot requires documented institutional authority, appropriate review and protection of student information. Assisted verification and authorized recovery should accommodate holders unable to use a wallet. Funding, conflicts, external assistance and author contributions must reflect actual circumstances and the receiving journal's requirements.

The principal limitation is the absence of an implemented, evaluated prototype. Synthetic workloads simplify governance and user behavior, and the focused review is not exhaustive. Key custody, source-record correctness and long-term archives remain institutional responsibilities. Future work should implement matched comparators, freeze acceptance policies, publish complete outcomes and then examine correction, recovery and verifier understanding in an authorized pilot. More advanced predicate and revocation mechanisms require separate validation.

IX. CONCLUSION

Academic credential verification needs appropriate disclosure, authentic issuer evidence, meaningful holder binding and sufficiently fresh status. The proposed design limits the ledger to shared governance and status commitments while retaining sensitive records outside routine replication. Its evaluation separates security, privacy, revocation and performance, allowing the ledger's added assurance to be judged against a strong conventional service before quantitative benefits are claimed.

REFERENCES

[1]. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, Article 30, 1–15. https://doi.org/10.1145/3190508.3190538

[2]. Barker, E. (2020). Recommendation for key management: Part 1—General (NIST Special Publication 800-57 Part 1, Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[3]. Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification

system. Sensors, 25(11), Article 3450. https://doi.org/10.3390/s25113450

[4]. Durant, E., & Trachy, A. (2017, October 17). Digital diploma debuts at MIT. MIT News. https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

[5]. Gupta, S. (2024). On-chain crypto-secured credential verification on permissioned blockchain. Proceedings of the 2024 IEEE International Conference on Blockchain and Distributed Systems Security, 1–6. https://research.google/pubs/on-chain-crypto-secured-credential-verification-on-permissioned-blockchain/

[6]. Hyperledger Fabric. (n.d.). The ordering service. Hyperledger Fabric documentation. Retrieved October 14, 2026, from https://hyperledger-fabric.readthedocs.io/en/latest/orderer/ordering_service.html

[7]. OpenID Foundation. (2025). OpenID for verifiable presentations 1.0 [Final specification]. https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html

[8]. Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

[9]. World Wide Web Consortium. (2025a). Bitstring Status List v1.0 [W3C Recommendation]. https://www.w3.org/TR/2025/REC-vc-bitstring-status-list-20250515/

[10]. World Wide Web Consortium. (2025b). Verifiable Credential Data Integrity 1.0 [W3C Recommendation]. https://www.w3.org/TR/2025/REC-vc-data-integrity-20250515/

[11]. World Wide Web Consortium. (2025c). Verifiable Credentials Data Model v2.0 [W3C Recommendation]. https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/

[12]. World Wide Web Consortium. (2026). Data Integrity BBS Cryptosuites v1.0 [W3C Candidate Recommendation Draft, September 10]. https://www.w3.org/TR/2026/CRD-vc-di-bbs-20260910/

About the Author:



(Srijib Samanta)
Assistant Professor and Head of Department (HOD)
Experience: More than 14 years
Department of Bachelor of Computer Application (BCA)
Tamralipta Institute of Management & Technology

Srijib Samanta is an Assistant Professor and Head of the Department of Bachelor of Computer Application at Tamralipta Institute of Management & Technology, with more than 14 years of experience.