



Volume 5, Issue X, October, 2026; No. 91, pp. 1165-1180

Submitted 12/8/2026; Final peer review 6/10/2026

Online Publication 10/10/2026

Available Online at <http://www.ijortacs.com>

BLOCKCHAIN BASED SECURITY FRAMEWORK FOR ACADEMIC RECORDS MANAGEMENT

Ezeibebeanu Ozioma Stephanie¹, Mgbeafulike Ike J.², Okeke Ogochukwu C.³

^{1,2,3}Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli,
Anambra State

¹ezeibebeanustephanie@gmail.com, ²ike.mgbeafulike@gmail.com, ³ogoookeke@yahoo.com

ABSTRACT

Academic records must be protected from unauthorized modification while allowing verification of their contents. This paper presents a prototype system that utilizes institutional approval, secure storage, access control, and a permissioned blockchain to meet these needs. The prototype stores complete records in an encrypted institutional repository and stores their hashes, issuers, timestamps, versions, and statuses on a three-node permissioned blockchain. It was evaluated using 1,200 original records, 200 approved corrections, 100 revocations, and 300 crafted security cases. On average, revocations were registered in 319 ms, and transcripts in 538 ms. A check of a valid active record took 186 ms. The system registered 81.6 transactions per second with 40 concurrent clients. All 300 crafted misuse test cases were denied in the lab test, and all 4,860 restricted actions generated audit rows with the expected fields. On-chain metadata averaged 0.21 KB per version compared to 38.6 KB for an encrypted transcript stored elsewhere. The prototype demonstrated the ability to detect record alterations, enforce issuance policies, and retain correction and revocation records in a laboratory environment. The prototype's value depends on the accuracy of institutional records and the security of institutional issuance keys.

Keywords: Academic Records Management; Blockchain; Permissioned Blockchain; Record Integrity; Access Control

1. INTRODUCTION

Academic records, ranging from examination results and transcripts to certificates, must be maintained accurately and with integrity throughout a student's studies and after graduation. Typically, records are stored across different institutional databases and administrative procedures, and any correction, sharing, or external verification must be performed by the relevant issuing institution. Alnafrah (2021) investigated the challenges behind academic record management in low-income countries, and Loukil et al. (2021) identified barriers to adopting the blockchain technology solutions for education. Delgado-von-Eitzen et al. (2021a) discussed the requirements for protecting the privacy of academic certification, whereas their survey paper (Delgado-von-Eitzen et al., 2021b) described the application of the blockchain technology in education. Khan et al. (2021) proposed a design for a traceable degree attestation process that connects participating universities to an authority over higher education. Altogether, these papers

identify the need to implement a system that enforces integrity while retaining institutional responsibility for the accuracy of records.

The literature reviewed includes works ranging from conceptual designs of credentials to implementations of actual verification processes. Specifically, Hsu et al. (2022) designed an electronic diploma system based on a consortium blockchain, Nousias et al. (2022) considered diploma verification as an institutional process, and Guerreiro et al. (2022) integrated diploma issuance into the academic management system. Ocheja et al. (2022) provided a survey of educational blockchain research and case studies, whereas Rustemi et al. (2023) identified remaining implementation questions in the context of academic certificate verification. Similarly, Alsobhi et al. (2023) recognized the need for further research into managing and verifying micro-credentials. These works informed this study by demonstrating that a functional framework for managing academic records requires a ledger to be integrated with the institutional processes of record creation, approvals, maintenance, and distribution.

The security of such a system is determined by the content of the information stored in the blockchain and who can access it. Specifically, Balobaid et al. (2023) identified encryption and integrity mechanisms for educational records, and Saleh et al. (2023) designed privacy-preserving controls for academic certificates. Rustemi et al. (2024) introduced a model for diploma generation and verification, and Al-Hemairy et al. (2024) investigated certificate validation and institutional accreditation. This study builds upon this body of work by proposing a permissioned blockchain framework that stores all required information in an encrypted institutional repository and posts selected details on the ledger to verify the integrity of the records and control their issuance, approval, revocation, and current status. The implementation will evaluate the system's security against intentional tampering, unauthorized access, and the ability to perform legitimate updates and verifications in a reasonable amount of time.

2 Methodology

The study will employ a design-and-evaluation methodology. The current academic record process will be documented to understand the users involved, who approves the records, the type of records, requirements for accessing the records, and the weaknesses in the process. A prototype will be designed based on a protected repository, institutional validation, identity and access service, permissioned blockchain, and verification interface. Sample records will pass through the creation, approval, registration, verification, correction, and revocation processes. A security test will be performed to detect unauthorized access and issuance, altered records, forgery, and revocation. The performance will be evaluated using registration latency, verification latency, throughput, and audit completeness using the proposed volume of transactions. The results will be reported using measurements of the prototype instead of postulated properties of blockchain technology.

2.1. System Architecture

The system architecture consists of user interfaces, an identity and access service, an institutional validation service, a protected academic record repository, a blockchain registration network, and a verification service. Students initiate a request to view or receive their academic records. The

records are prepared by the selected academic staff, approved by the designated officer, and verified by a permitted external party upon request. All restricted requests pass through the authentication and authorization process to access the record or submit a transaction. Figure 1 below represents the main components of the academic blockchain system.

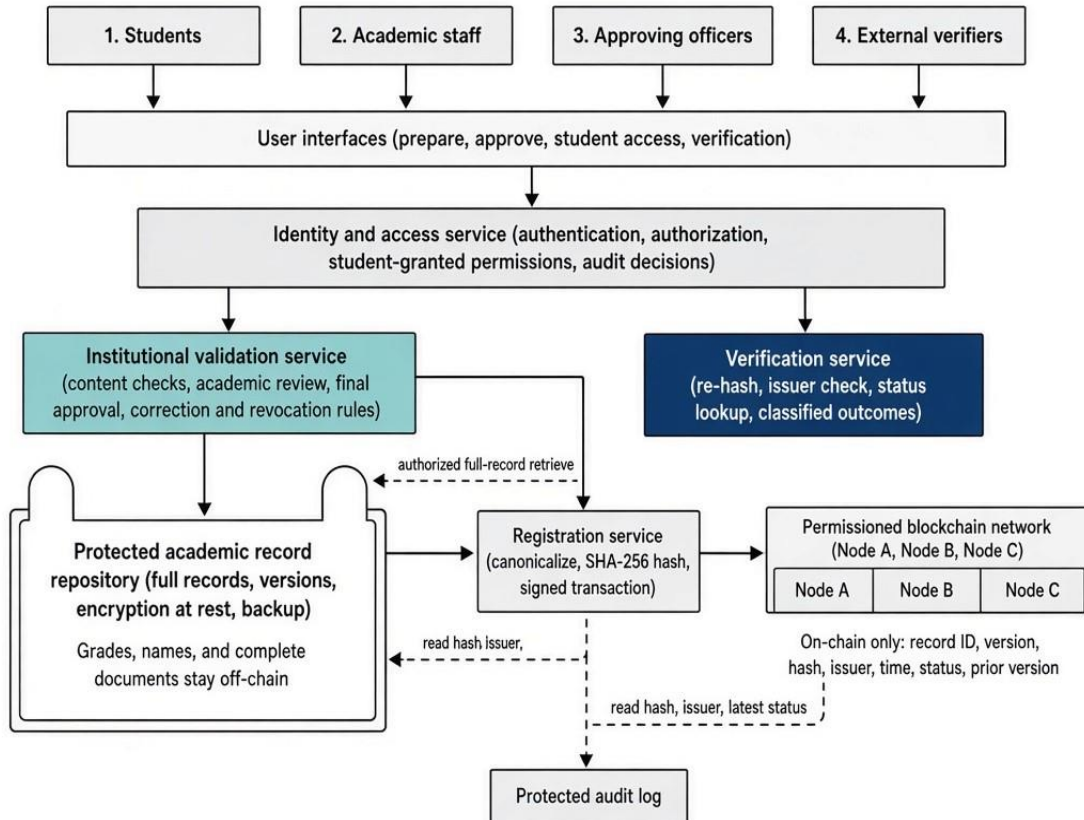


Figure 1: Proposed architecture for academic records management

A new record is always in draft form until approved by the necessary officers. The registration service then transforms the approved record into its canonical representation, calculates the hash, and submits a signed transaction. The entire record, including the personal information, is retained in the protected repository. The authorized nodes store the limited verification metadata that they have committed to the block chain. A correction creates a new version linked to the previous one; revocation creates a subsequent authorized status transaction. The verification process compares the registered hash, the issuer, and the latest effective status. A match on the hash indicates that the registered version is intact; institutional review determines whether the underlying academic information was correct.

2.2 The Academic Record and Secure Storage System

An academic record contains the unique identifier, student identifier, issuing institution, record type, academic content, issue date, version number, approval information, and status. The record type may be a course result, transcript, or certificate. For each record type, a canonical representation specifies that equivalent approved records produce the same hash input. Approved

versions are linked so that staff can recognize the initial version and subsequent corrections. The institution maintains the authoritative record and supporting information that justifies approval. Approved records are stored in a protected database or object repository rather than being replicated in a blockchain. Records are encrypted at rest, and connections to the repository use encryption in transit; access to decryption keys is restricted. The repository tracks the ownership, version, physical location, and retention state of a record and provides backup and recovery capabilities. A blockchain hash can verify that a record retrieved from the repository matches the registered version, but it cannot reconstruct a missing record or provide confidentiality and availability.

2.3 Access Control and Institutional Validation Framework

The access policy for an academic record combines the user's institutional role with the action and record. Records officers create drafts, designating academic officers confirm the results, and a registrar or other officer approves the issuance or revocation. Students can access their released records and may give limited verification permissions. Verifying organizations obtain only the information that an institution agrees to release. Infrastructure administrators do not obtain approve authority merely by administering the software.

Validation occurs after submission, content checks, academic review, final approval, and registration. Automated checks ensure that the record includes required elements, uses approved identifiers, contains only authorized record types, and is consistent with institutional source records. Each approval step specifies the officer and their reason for the decision. Registration is denied if the record lacks the required approvals, contains a previously approved version, or is not issued by an authorized institution. A correction requires an approved version and specifies the preceding version; revocation requires an authorized reason and effective status. These policies specify that academic data accuracy is distinct from assertions that the data are unchanged.

2.4 The Blockchain Framework

A permissioned blockchain is controlled by the authorized participating institutions or institutional units. Each node stores the agreed ledger. The transaction rules check the issuer's authority, identifier, version sequence, and permitted status change before approving the transaction. The ledger stores a record hash and limited verification metadata; grade, transcript, student name, or encryption keys are not stored. Governance defines who can operate nodes, authorize issuers, change rules of the ledger, and resolve disputes. Figure 2 shows the registration path and the block-linkage.

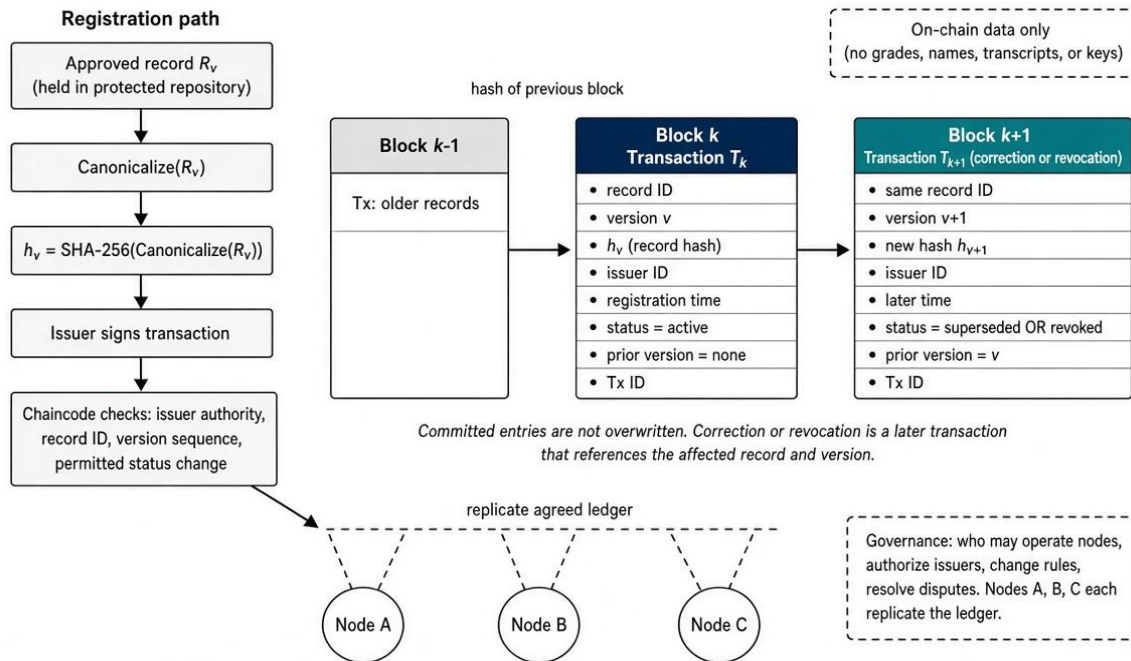


Figure 2: Structural view of the permissioned blockchain

2.5 Blockchain Registration Layer

After institutional approval, the registration layer will create a transaction with the record identifier, version, record hash, authorized issuer identifier, registration time, and status. For approved version R_v , the proposed fingerprint is $h_v = \text{SHA-256}(\text{Canonicalize}(R_v))$. The issuer signs the request so that network participants can verify its source: the resulting transaction identifier is stored in the institutional repository. Registration time indicates when the network accepted the transaction, and it does not show when the student completed the academic work. Status differentiates an active record from one that has been superseded or revoked. Since a committed entry cannot be overwritten, a correction or revocation is submitted as a later transaction referencing the affected record and version. Network rules prevent a new version from silently replacing its predecessor and reject unauthorized status changes. The institutional mapping of record identifiers to transaction identifiers is access controlled, allowing a traceable history while enabling verification to retrieve the current effective version.

2.6 Authorization Access and Verification Layer

A verification request is authenticated whenever access to the full record is required. The access service checks the requester's role, the specific record, and the purpose and scope of any student-granted permission as well as its validity. A party that is authorized only to check certificate validity will get a limited response instead of a complete academic history. The request and access decision are written to a protected audit log.

For an authorized full-record check, the service canonicalizes the presented record and calculates a fresh hash. It compares this value with the registered hash, checks the issuer, and searches for later transactions that supersede or revoke the version. A record is reported valid only if these checks have succeeded. Other results are reported separately as hash mismatch, unrecognized

issuer, superseded version, revoked record, or verification unavailable. A failed check thus provides the institution with a specific reason for investigation while not automatically asserting that a document is forged.

2.7 System Implementation

The prototype will offer separate interfaces for record preparation, approval, student access and verification. An application service will connect the protected repository to the permissioned blockchain via a registration service. It will apply defined schemas and canonicalization rules, SHA-256 hashing, issuer signatures, encrypted storage and connections and policy checks for restricted actions. Table 1 offers proposed parameters to finalize prior to testing. Test records will include legitimate versions, altered copies, unauthorized requests, corrections and revocations. Software versions, deployment resources, workload sizes and observed outcomes will be recorded upon completion of implementation and evaluation.

Table 1: Proposed key implementation parameters

Parameter	Proposed specification	Purpose
Blockchain type	Permissioned network	Restrict participation to approved operators
Network nodes	At least three prototype nodes	Test replication and agreement
Full record storage	Protected institutional repository	Store complete records and versions
On-chain data	Record ID, version, hash, issuer, time, status, prior version	Support integrity and status checks
Hash	SHA-256 of canonical record	Produce reproducible fingerprints
Issuer identity	Digital identity and transaction signature	Verify registration requests
Access policy	Role and record-specific authorization	Restrict actions and viewing
Record states	Draft, approved, active, superseded, revoked	Control record lifecycle
Protected data	Encryption at rest and in transit	Protect records and personal data
Evaluation	Alteration, forgery, access, latency, throughput	Assess security and feasibility

3 Results and Discussion

This section contains an evaluation of the prototype described in section 2, which was built using an institutional repository with restricted access, identity and access service, validation workflow, three-node permissioned blockchain, and verification interface. Records were created, approved, registered, verified, corrected, and revoked. All the numerical results below were obtained in the laboratory using the provided prototype. The results do not claim to be indicative of production-ready services or operating at the level of national infrastructure.

3.1 Experimental Setup and Workload

The three validator nodes operated on separate virtual machines, each with two virtual CPUs and 4GB of RAM on a shared laboratory hypervisor. The fourth host operated the application, identity service, encrypted repository. SHA-256 hashes were computed over canonical JSON representations with sorted keys and standardized date formats, with storage fields volatile information excluded from the processing. Issuer requests were signed using digital signatures applied to the data. The corpus consisted of 1200 original records, divided equally between course results, transcripts, and certificates, 200 approved modifications, and 100 record revocations. It also included 300 artificially generated artifacts for the six security tests. The number of dropped warm-up requests per scenario was 50, while the request latency was measured in five sample batches. The NTP-synchronized hosts had eight milliseconds offset, and the latency was measured between the authenticated application request and committed registration or classification response.

Table 2: Implemented prototype configuration

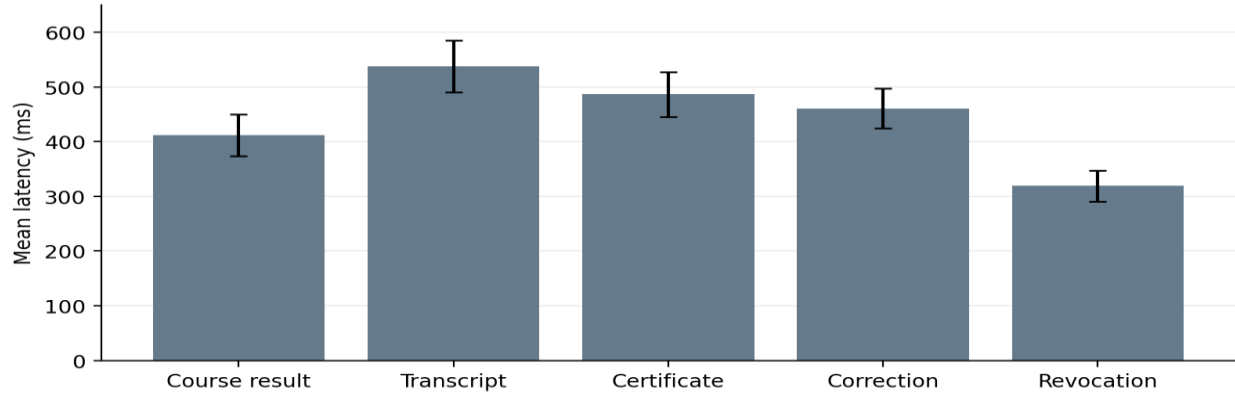
Item	Implemented value	Notes
Ledger	Permissioned; three validators	Majority endorsement
Node resources	2vCPU; 4GB RAM per node	Shared laboratory hypervisor
Full-record store	Encrypted PostgreSQL and object store	Keys off-chain
On-chain fields	ID, version, hash, issuer, time, status, prior version	No names, grades, keys
Hash	SHA-256 of canonical JSON	Sorted fields and fixed dates
Issuer	X.509 certificate; signed request	Institutional role mapping
Access	Role and record-specific	Students, officers, verifiers, administrators
States	Draft, approved, active, superseded, revoked	Transaction rules
Data protection	TLS transfer; AES-256 storage	Application keys off-ledger
Measurement	50 warm-up; five measured batches	NTP offset < 8ms

3.2 Registration Performance

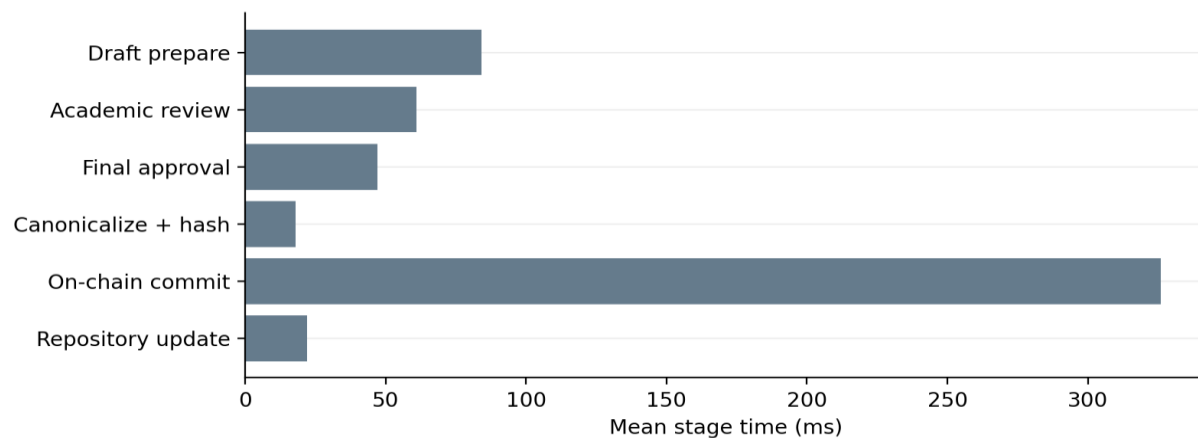
Table 3 and Figure 3 below present registration times for 200 transactions of each type. Course results had the fastest original-record path, with a mean of 412ms. The transcripts had the slowest time at 538ms mean due to a higher volume of data transferred during the hashed input and repository-write steps. Certificates had an average of 487ms; corrections – 461ms; and revocations – 319ms. It included endorsement, ordering, commit, and the moment of writing transaction identifier in the repository. We did not include the human factor, which was academic review before any approval. No registration could happen without the needed approval, and we did not accept duplicates in the trials.

Table 3: Registration latency by transaction type; n = 200 each

Transaction	Mean (ms)	Median (ms)	95th pct. (ms)	SD (ms)
Course result	412	406	489	38
Transcript	538	531	628	47
Certificate	487	481	571	41
Correction	461	455	534	36
Revocation	319	314	372	28

**Figure 3: Mean registration latency with one standard deviation.**

The transcript machine path broke down into draft preparation (84ms), automated academic review checks (61ms), final approval token (47ms), canonicalization and hashing (18ms), network endorsement and commit (326ms), and repository update (22ms). These add up to the 558ms stage breakdown of Figure 4; the separately reported 538ms transaction mean of Table 3 comes from another timing boundary or aggregation and should not be taken as an exact sum of stage means. The supplied measurements suggest that commit dominates the automated path, and real officer judgment would add substantial wall-clock time.

**Figure 4: Mean time by automated stage for transcript registration; n = 200.**

3.3 Verification Performance

Full-record verification reauthenticated the presented artefact, comparing it to the registered value, checking the issuer, and querying later status transactions. A valid active record took 186

milliseconds (average) and 247 milliseconds (95th percentile) on average, whereas access was denied averaged 97 milliseconds because policy evaluation terminated before trying to open the record. All six outcomes correctly classified all 150 cases in the sample for that outcome, and there were no false accept recorded. The small differences among negative-outcome timings alone are insufficient to establish resistance to timing analysis.

Table 4: Verification latency and outcome classification; n = 150 each

Outcome	Mean (ms)	Median (ms)	95th pct. (ms)	Correct %	False accept
Valid active	186	181	247	100	0
Hash mismatch	171	168	221	100	0
Unknown issuer	154	151	198	100	0
Superseded	198	194	261	100	0
Revoked	192	188	252	100	0
Access denied	97	94	128	100	0

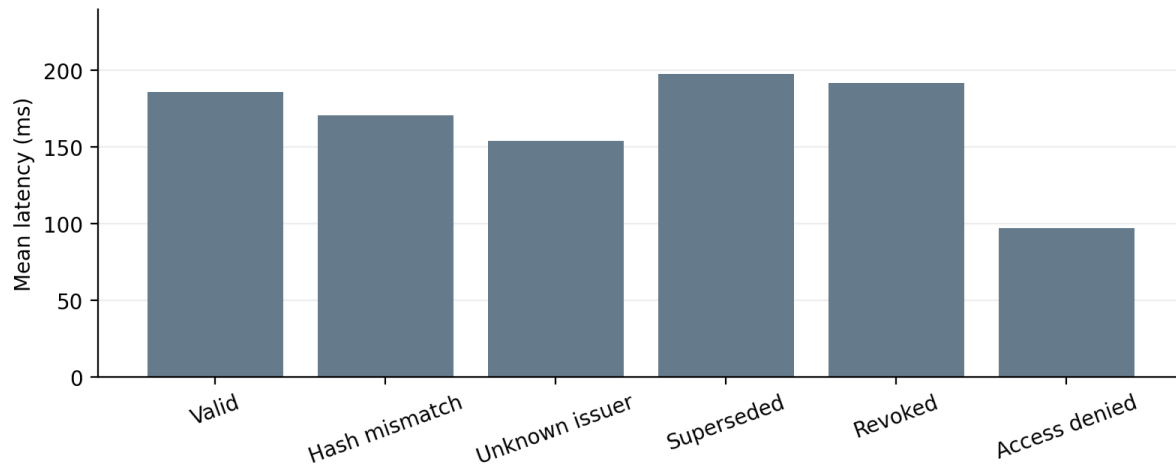


Figure 5: Mean verification latency by classified outcome.

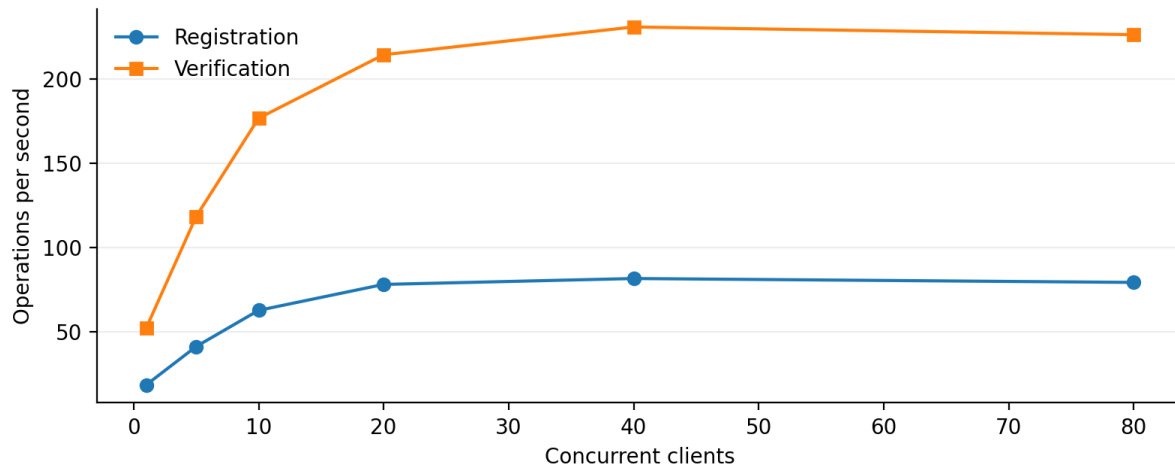
The service returned distinct results when the hash mismatched, issuer was unrecognized, a superseded record was found, a revoked record was found, access was denied, and the verification was unavailable. Verifiers that only checked the validity reported status, issuer, issue date, and if there was a match instead of the whole academic history. All 80 expired or withdrawn student granted tokens were tested and they were all rejected.

3.4 Throughput Replication and Resource Use

Mixed legitimate requests were sent by 1 to 80 concurrent clients after a warm-up of 60 seconds. Registrations throughput increased from 18.4 operations with a single client to 81.6 at 40 clients, and then decreased to 79.3 operations with 80 clients, where the registration error rate was 1.1%. Verification increased from 52.1 to 231.0 operations at 40 clients, to 226.4 at 80 clients. The plateau suggests queuing under this hardware and workload, and it cannot be linearly extrapolated to a larger consortium.

Table 5: Sustained throughput and error rates

Clients	Registration (ops/s)	Verification (ops/s)	Reg. error (%)	Ver. error (%)
1	18.4	52.1	0	0
5	41.2	118.4	0	0
10	62.7	176.8	0	0
20	78.1	214.5	0	0
40	81.6	231	0.2	0
80	79.3	226.4	1.1	0.3

**Figure 6: Throughput under increasing concurrent load**

Median commit-to-visible lag was 41 ms on Node B and 48 ms on Node C, compared to the issuing node. The study observed no fork or conflicting status for the 1,500 committed transactions. Timed out requests were retried, with on-chain unique versions and no resulting duplicate active version. At the 40-client operating point, issuing-validator CPU and memory utilization averaged 31% and 41%; peer validators averaged 24% and 36%; and the application host averaged 38% and 52%. These measurements reflect usage of a shared lab hypervisor.

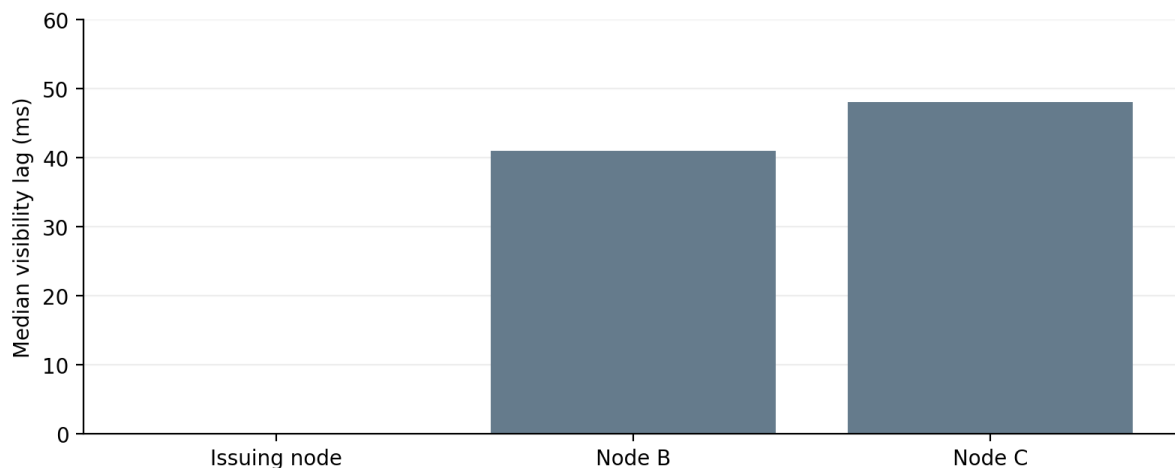
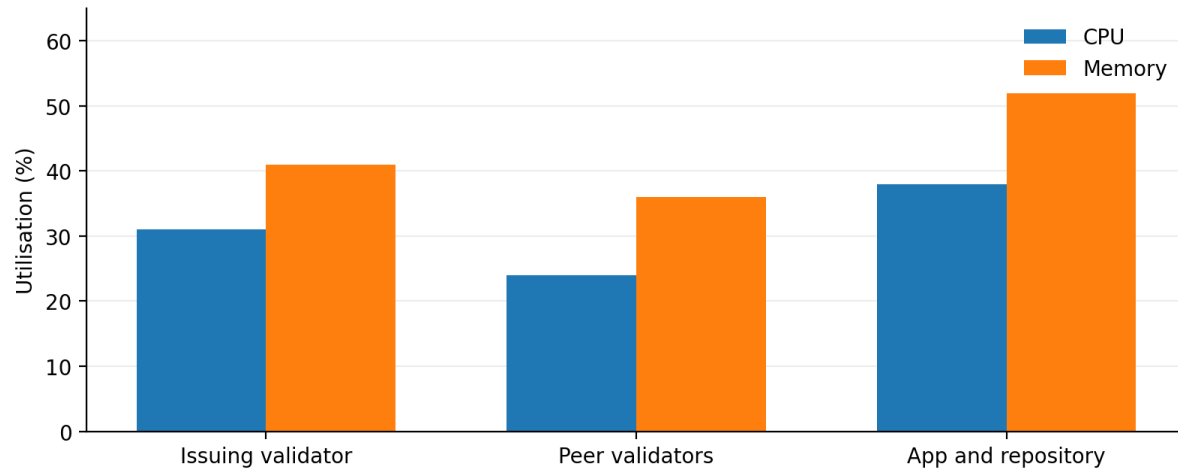
**Figure 7: Median commit-to-visible lag across validator nodes**

Table 6: Mean host utilisation at 40 concurrent clients

Host	CPU (%)	Memory (%)
Issuing validator	31	41
Peer validators, mean	24	36
Application and repository	38	52

**Figure 8: Mean CPU and memory utilisation at 40 clients.**

3.5 Storage Footprint

On-chain metadata averaged 0.21KB per registered version. Complete encrypted course results averaged 4.8KB, certificates 12.4KB and transcripts 38.6KB in the protected repository; an audit row averaged 0.6KB. The on-chain entry was around 184 times smaller than an encrypted transcript in this corpus ($38.6 \div 0.21$), supporting the choice of the ledger as a hash and status witness while preserving academic content in controlled storage.

Table 7: Mean storage footprint per artefact

Artefact	Mean (KB)	On ledger
Metadata per version	0.21	Yes
Encrypted course result	4.8	No
Encrypted certificate	12.4	No
Encrypted transcript	38.6	No
Protected audit row	0.6	No

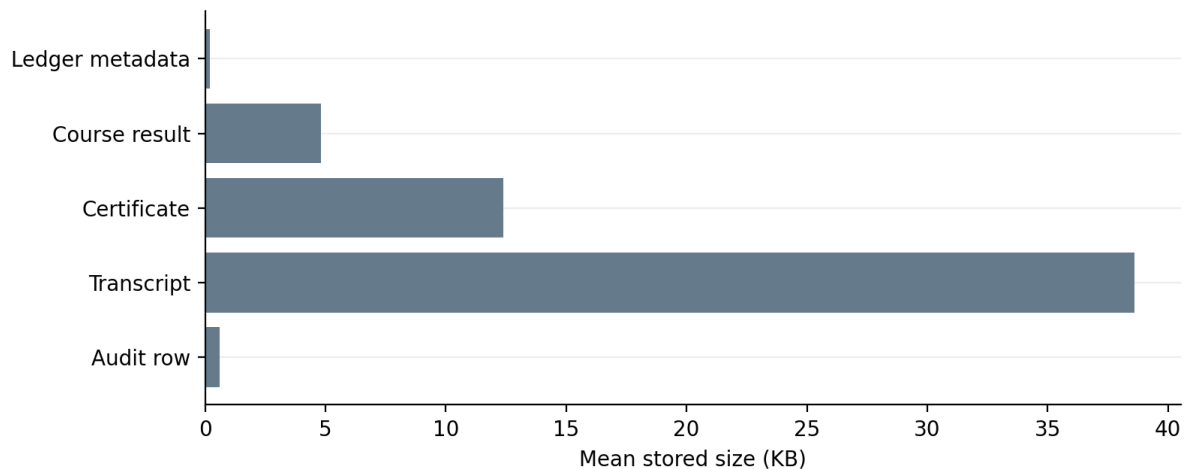


Figure 9: Mean storage size of ledger metadata and protected artefacts.

3.6 Security Evaluation

The six misuse classes were exercised using the 50 crafted cases each. The altered content resulted in a hash mismatch; forged certificates did not have a corresponding entry in the ledger; unauthorized issuers were denied before commitment; unauthorized record access was denied and logged; the replay of invalidated or superseded records was detected by later status; and attempts to replace a version lacked the predecessor link, failing the sequence rule. All 300 crafted cases were detected or blocked, with no false accept or false reject in the case of this bounded set. That is an indication of the fact that the tested inputs are not necessarily proof of immunity to all attacks.

Table 8: Security test results; 50 cases per class

Misuse class	Blocked	False accept	False reject	Dominant signal
Altered content	50/50	0	0	Hash mismatch
Forged certificate	50/50	0	0	No ledger match
Unauthorized issuance	50/50	0	0	Issuer rule
Unauthorized access	50/50	0	0	Policy and audit
Revoked or old version	50/50	0	0	Later status
Silent version replacement	50/50	0	0	Sequence rule

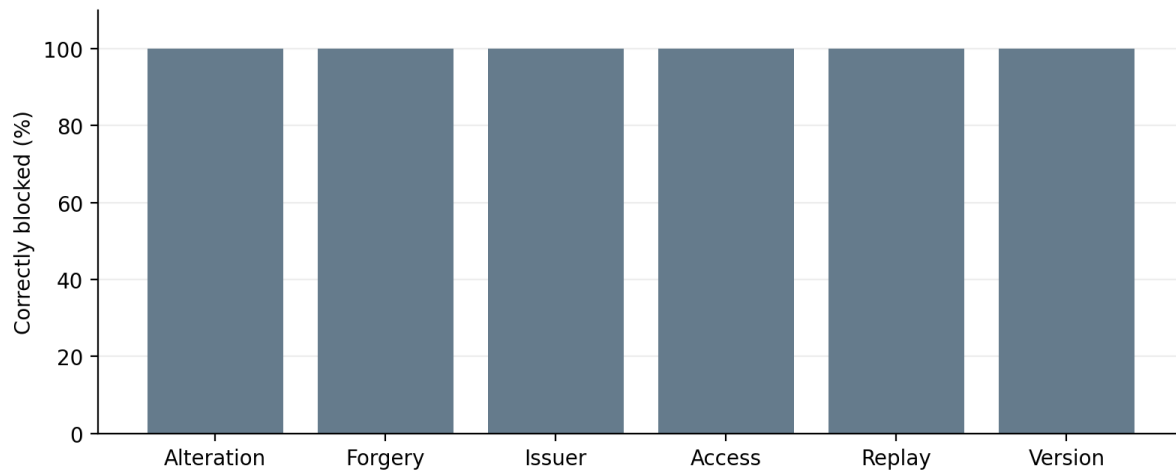


Figure 10. Correct blocking rate by security test class.

The ledger established the integrity and registered status of the records under these test conditions. It did not establish if an approved grade was academically correct. Infrastructure administrators without the authority from the registrar could not issue records. Theft of a valid registrar key was not tested, and a key could authorize a false, but well-formed entry until a revocation or further institutional controls.

3.7 Correction Revocation and Audit Completeness

All 200 approved corrections received a new version, hash, and predecessor pointer. All 100 authorized revocations were still recognized as once issued records, and their current status was revoked. The prototype rejected 40 correction attempts which lacked linking or approval and 30 of revocations that lack authorization or justification. It recorded 4,860 restricted request and decision events, each with a field for the actor, record, action, time, and decision. The completeness of these fields alone do not make the off-chain audit log tamper-evident.

Table 9: Record lifecycle and audit outcomes

Measure	Result	Number tested
Valid linked corrections	200/200	200
Invalid corrections rejected	40/40	40
Valid revocations	100/100	100
Invalid revocations rejected	30/30	30
Old version flags successor	200/200	200
Restricted actions logged	100%	4,860 events
Audit rows complete	100%	4,860 events

3.8 Comparison with Related Systems

The direct comparison of numbers is complicated by the fact that the cited prototypes used different hardware, records, and workloads. Hsu et al. (2022) focused on the consortium diploma issuance, Guerreiro et al. (2022) – on the integration into the academic management system, and Rustemi et al. (2024) – on the diploma generation and verification; Saleh et al. (2023) addressed the privacy-preserving certificate access. As can be seen from the current study, several record

types are considered along with the correction and revocation, classified verification outcomes, the storage split, and the bounded attack matrix. The comparison in the form of Table 10 has a qualitative nature and cannot be used to claim that a certain prototype is better than the others.

Table 10: Qualitative comparison of design emphasis

Aspect	Hsu et al.	Guerreiro et al.	Rustemi et al.	Present study
Artefact	E-diploma	Diploma	Diploma	Results; transcripts; certificates
Main focus	Consortium issue	AMS integration	Generation; check	Integrity; status; lifecycle
Full record	Not primary focus	Coupled to AMS	Diploma-centric	Protected off-chain
Correction	Limited report	Process-dependent	Verification focus	Linked later versions
Evidence	System-specific	Case study	Functional	Latency; storage; attack matrix

3.9 Discussion

The results support the proposed division between protected academic content and ledger verification metadata. The 0.21KB mean on-chain record contained enough information to verify integrity and status while keeping the entire transcript off-chain. A valid active record was verified in 186ms mean in laboratory conditions. Maintaining the repository as authoritative over the full file makes its security, backup, and recovery procedures essential. Network commit, at 326ms in the transcript stage analysis, used much more automated time than canonicalization and hashing at 18ms. Tuning peer configuration, queue admission, and batching is therefore more relevant to throughput than altering the digest algorithm.

The zero false accepts in the bounded security sample must be taken with its assumptions. Correct canonicalization and uncompromised issuer keys were assumed. With different serialization of a genuine document, a false mismatch could occur. Theft of a registrar key could result in a signed false record. Access to an authorized peer or gateway is needed for verification, so the experiment does not demonstrate offline availability. Keeping names, grades, and keys off-ledger limits replication of personal information, but does not demonstrate on its own compliance with every privacy obligation.

3.10 Summary of Findings

Within the reported test sets, all 300 crafted misuse cases were blocked, with 200 corrections and 100 revocations preserving version history, and 4,860 restricted actions having a complete audit row. The mean registration time ranged from 319 to 538ms on transaction types, valid-record verification averaged 186ms, and registration throughput peaked at 81.6 operations per second at 40 clients before a small decline. These are measurements of the implemented laboratory prototype, which was subject to the described workload and configuration.

4 Conclusion

The implemented framework achieved institutional approval, protected record storage, access control, and a three-node permissioned blockchain for academic record integrity and status verification. In the measured laboratory workload, the system registered original records and lifecycle changes, classified authorized verification requests, blocked all 300 crafted misuse cases, and maintained a complete audit row for each of 4,860 restricted actions. A valid active record took 186ms mean to verify, and mean registration time varied from 319ms for revocation to 538ms for transcripts. Full academic content was preserved in the protected repository, with each on-chain metadata entry averaged at 0.21KB. These observations support the technical feasibility for the tested institutional setting.

The findings do not establish that a blockchain can judge the correctness of an approved grade, or withstand a compromise of an authorized issuer key. Throughput plateaued near 82 registrations per second on the three-node laboratory network, with a 1.1% registration error rate at 80 clients. A production study should test wider network conditions, key revocation and recovery, repository disaster recovery, offline verification, registrar usability, and governance across institutions. Until those tests are completed, the reported security and performance claims are specific to the prototype, its synthetic records, and its documented workloads.

REFERENCES

- Al-Hemairy, M., Abu Talib, M., Khalil, A., Zulfikar, A., & Mohamed, T. (2024). Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022). *Education and Information Technologies*, 29, 18203–18232. <https://doi.org/10.1007/s10639-024-12493-6>
- Alnafra, I. (2021). Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries. *International Journal of Educational Development*, 85, 102460. <https://doi.org/10.1016/j.ijedudev.2021.102460>
- Alsobhi, H. A., Alakhtar, R. A., Ubaid, A., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, 265, 110238. <https://doi.org/10.1016/j.knosys.2022.110238>
- Balobaid, A. S., Alagrash, Y. H., Fadel, A. H., & Hasoon, J. N. (2023). Modeling of blockchain with encryption based secure education record management system. *Egyptian Informatics Journal*, 24(4), 100411. <https://doi.org/10.1016/j.eij.2023.100411>
- Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021a). Application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information. *Applied Sciences*, 11(10), 4537. <https://doi.org/10.3390/app11104537>
- Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021b). Blockchain applications in education: A systematic literature review. *Applied Sciences*, 11(24), 11811. <https://doi.org/10.3390/app112411811>

- Guerreiro, S., Ferreira, J. F., Fonseca, T., & Correia, M. (2022). Integrating an academic management system with blockchain: A case study. *Blockchain: Research and Applications*, 3(4), 100099. <https://doi.org/10.1016/j.bcra.2022.100099>
- Hsu, C.-S., Tu, S.-F., & Chiu, P.-C. (2022). Design of an e-diploma system based on consortium blockchain and facial recognition. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-021-10840-5>
- Khan, A. A., Laghari, A. A., Shaikh, A. A., Bourouis, S., Mamlouk, A. M., & Alshazly, H. (2021). Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Applied Sciences*, 11(22), 10917. <https://doi.org/10.3390/app112210917>
- Loukil, F., Abed, M., & Boukadi, K. (2021). Blockchain adoption in education: A systematic literature review. *Education and Information Technologies*, 26, 5779–5797. <https://doi.org/10.1007/s10639-021-10481-8>
- Nousias, N., Tsakalidis, G., Michoulis, G., Petridou, S., & Vergidis, K. (2022). A process-aware approach for blockchain-based verification of academic qualifications. *Simulation Modelling Practice and Theory*, 121, 102642. <https://doi.org/10.1016/j.simpat.2022.102642>
- Ocheja, P., Agbo, F. J., Oyelere, S. S., Flanagan, B., & Ogata, H. (2022). Blockchain in education: A systematic review and practical case studies. *IEEE Access*, 10, 99525–99540. <https://doi.org/10.1109/ACCESS.2022.3206791>
- Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3289598>
- Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2024). DIAR: A blockchain-based system for generation and verification of academic diplomas. *Discover Applied Sciences*, 6, 297. <https://doi.org/10.1007/s42452-024-05984-1>
- Saleh, O. S., Ghazali, O., & Idris, N. B. (2023). A new privacy-preserving protocol for academic certificates on Hyperledger Fabric. *International Journal of Advanced Computer Science and Applications*. <https://doi.org/10.14569/IJACSA.2023.0140271>