Ngr. J. Multi. vol-2, issue-9 (Sep-2026) pp-529-541

ISSN: 3108-2750 (E), 3139-8065 (P)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/index.php/ngrjm/index

Research Article

Development and Evaluation of a Prototype Dlt-Based Credential Management System

Samuel C. Onyebuchi-Igbokwe [1]*, Eugevar D. Silang[2]

[1-2] Masters Student, MIT, University of Luzon, Pangasinan, Philippines

ABSTRACT:

The digital transformation of higher education has created an urgent need for transparent, efficient, and verifiable management of student records. Traditional centralized systems for credential management rely heavily on Trusted Third Parties (TTPs), creating vulnerabilities related to data integrity, ownership, and single points of failure. This study aimed to design, develop, and evaluate a prototype decentralized ledger technology (DLT)-based credentialing system called "The Consortium" for educational and employment applications. The researcher employed a Design Science Research approach combined with Agile software development methodology. The system was built using a modern web technology stack including Next.js 16, React 19, TypeScript, and cryptographic libraries to simulate a consortium blockchain environment. The system implements a three-role architecture involving Holders (Students), Issuers (Universities), and Verifiers (Employers). Key security features include Decentralized Identifiers (DIDs), SHA-256 hashing for multi-document portfolio integrity, and HMAC-SHA256 digital signatures for credential verification. Thirty purposively selected respondents (15 Holders, 5 Issuers, and 10 Verifiers) evaluated the prototype using a researcher-constructed questionnaire based on ISO/IEC 25010 quality characteristics. The prototype successfully eliminated the need for intermediaries by enabling instant, trustless verification of credentials. Verification speed tests showed completion in under 200 milliseconds compared to 5-10 business days for traditional methods. The system demonstrated 100% success in recording all eight transaction types (DID registration, portfolio submission, portfolio rejection, verifiable credential issuance, credential revocation, credential forwarding, credential decision, and chat messaging) with no duplicate hashes. Tampering detection tests confirmed that any modification to portfolio documents immediately produced different hash values, ensuring integrity. The usability evaluation yielded mean scores of 4.4 for ease of use, 4.6 for speed perception, and 4.5 for trust, with an overall mean of 4.5 out of 5.0, all interpreted as "Strongly Agree." The Consortium prototype confirms the viability of DLT in reducing credential fraud and administrative inefficiency in the education sector. The system enables students to maintain self-sovereign ownership of their records while providing institutions with a secure, tamper-proof method of issuance, verification, and revocation. Future work should focus on controlled deployment on a permissioned test network, smart contract migration, and integration with institutional record systems.

Keywords: Decentralized Ledger Technology (DLT), Blockchain, Decentralized Identity (DID), Verifiable Credentials, Cryptography

Citation: Onyebuchi-Igbokwe, S. C., & Silang, E. D. (2026). Development and evaluation of a prototype DLT-based credential management system. *Nexus Global Research Journal of Multidisciplinary, 2*(9), 529–541.

1. INTRODUCTION

1.1 Background

The digital transformation of higher education has emphasized the need for transparent, efficient, and verifiable management of student records and credentials. As educational institutions continue to adopt e-learning and digital assessment tools, the electronic portfolio (e-portfolio) has emerged as a vital tool for demonstrating students' learning achievements. However, most existing e-portfolio and credential management systems remain centralized, operating within institutional boundaries and dependent on Trusted Third Parties (TTPs) for verification.

According to the Commission on Higher Education (CHED), educational credential fraud remains a systemic risk in the Philippines. Furthermore, centralized systems introduce a single point of failure (SPF) where records can be unilaterally modified or lost. The integration of blockchain technology offers a solution through distributed ledgers that record transactions in immutable, cryptographically linked blocks.

This project, which the researcher calls "The Consortium," aims to design and simulate an Inter-Institutional Blockchain Platform for Student

***Corresponding Author:** Samuel C. Onyebuchi-Igbokwe, **Email:** blackkiverson@gmail.com

Received: 10 Aug 2026 | **Accepted:** 05 Sep 2026 | **Published:** 16 Sep 2026

Copyright © 2026 The Author(s): This work is licensed under a Creative Commons Attribution- Non-Commercial-No Derivatives 4.0 (CC BY-NC-ND 4.0) International License

Lifecycle Management, emphasizing secure, decentralized credential issuance, verification, revocation, and stakeholder communication using the latest web and cryptographic technologies.

In the context of this project, "The Consortium" refers to a permissioned blockchain network where control is shared among a pre-approved set of nodes—such as a group of universities or organizations—working together to issue verifiable academic credentials, verify those credentials without contacting the original institution, revoke credentials when necessary, and forward credentials between parties (e.g., Students to Employers).

The three key parties that form the consortium are:

- **Holders (Students):** Who own and manage their credentials
- **Issuers (Universities/Organizations):** Who sign and mint verifiable credentials
- **Verifiers (Employers/Organizations):** Who authenticate credentials

Together, these three roles constitute the "Trust Triangle," a foundational architectural model in which trust is established through cryptographic proofs and verifiable data exchanges rather than institutional authority.

1.2 Statement of the Problem

The researcher aimed to develop and evaluate a prototype DLT-based credential management system tailored specifically for education and employment. Specifically, this study sought to address the following questions:

1. What design architecture can be used to develop a DLT-based prototype for secure credential issuance and verification?
2. What security features are needed to ensure credential integrity, authenticity, and user-controlled management within the prototype?
3. What is the level of acceptability and performance of the developed prototype in credential verification compared to traditional methods?

1.3 Significance of the Study

For Students (Holders):

The system grants complete ownership over educational data, facilitates professional mobility through portable credentials, and provides a digital wallet with credential forwarding, cover letter support, and real-time status tracking of submissions (pending, verified, rejected, revoked).

For Institutions (Issuers):

The system reduces administrative burden through streamlined portfolio review, supports typed credentials with metadata and expiry, provides credential revocation capabilities, and protects institutional reputation by preventing fraud.

For Employers (Verifiers):

The system enables near-real-time verification of applicant claims without contacting the issuing university, supports accept/decline decision recording with notes, and provides a complete audit trail of verification activities.

1.4 Scope and Delimitation

This study focuses on the architectural design and development of a functional prototype for a distributed ledger technology (DLT)-based credentialing system, featuring three distinct user portals—Holder (Student), Issuer (University), and Verifier (Employer). The system implements a cryptographic layer using SHA-256 for document hashing and HMAC-SHA256 for digital signatures, alongside a mock blockchain service that simulates a distributed ledger to record eight transaction types: DID registration, portfolio submission, portfolio rejection, verifiable credential (VC) issuance, VC revocation, credential forward, credential decision, and chat message.

Full credential lifecycle management is supported, including credential types, metadata, expiry dates, issuer notes, attachments, and revocation. The prototype also includes a ledger explorer for comprehensive transaction viewing with filtering by type and DID search, plus ledger reset functionality, and an in-app messaging system enabling context-aware chat between participants.

The study utilizes a "Mock Blockchain Service" (a local simulation of ledger logic) rather than a live deployment on a public mainnet to avoid gas costs during the development phase. The system does not currently integrate with legacy university databases but demonstrates the DLT logic required for such integration.

2. LITERATURE REVIEW

2.1 Design Architecture for DLT-based Systems

Blockchain technology has emerged as a transformative architecture for secure data management, particularly in environments requiring transparency, immutability, and decentralized trust. In educational credential systems, blockchain

architectures are increasingly utilized to address issues related to credential fraud, delayed verification, data tampering, and centralized dependency.

A consortium blockchain architecture is particularly suitable for educational credential verification systems because it allows multiple trusted institutions to participate in maintaining and validating ledger transactions while preserving controlled access to sensitive information. Unlike public blockchains, consortium blockchains restrict participation to authorized entities, making them more appropriate for academic and employment environments where governance, privacy, and institutional accountability are important.

Research by Sharples and Domingue (2016) proposed a blockchain-based framework for storing educational achievements and academic records in a distributed environment, demonstrating that blockchain technology can support decentralized trust by enabling credentials to be verified independently without requiring continuous involvement from issuing institutions. Similarly, Chen *et al.*,(2018) investigated blockchain applications in educational ecosystems and found that distributed ledger architectures improve data integrity, transparency, and interoperability among institutions.

A systematic review by Alammary *et al.*,(2019) analyzed blockchain applications in education and identified credential verification as one of the most common use cases. Their findings showed that blockchain architectures improve trustworthiness, traceability, and security in academic credential management, with consortium blockchain architectures being particularly suitable for educational institutions because they balance decentralization with governance and privacy control.

More recent research by Ismail *et al.*,(2024) and Kumar *et al.*,(2024) confirmed these findings, demonstrating that consortium blockchain models provide improved efficiency, controlled access, and institutional accountability while maintaining decentralized verification capabilities.

2.2 Security Features for DLT-based Systems

Cryptographic security mechanisms serve as the foundation of blockchain-based credential systems. Hashing algorithms, digital signatures, and decentralized identifiers are widely implemented to ensure credential integrity, authenticity, non-repudiation, and user-controlled identity management.

Hashing Algorithms:

SHA-256 is among the most commonly implemented hashing algorithms in blockchain environments because of its strong collision resistance and computational reliability. Research by Tariq *et al.*,(2024) demonstrated that SHA-256 hashing effectively protects digital credentials from unauthorized modification by generating tamper-evident representations of credential data, where any alteration immediately changes the hash value, enabling rapid detection of tampering.

Digital Signatures:

Through asymmetric cryptography, issuers sign credentials using private keys, while verifiers validate signatures using corresponding public keys. Research indicates that digital signature implementations significantly reduce fraudulent credential issuance and eliminate the need for repetitive manual authentication procedures (Ismail et al., 2024).

Decentralized Identifiers (DIDs):

Research by Naik and Jenkins (2020) emphasized that DIDs enable individuals to maintain ownership and control over their digital identities without dependence on centralized authorities. Studies revealed that DID-based systems improve user autonomy while reducing risks associated with centralized identity storage, making them highly suitable for educational and employment verification environments.

2.3 Evaluation of Performance and Usability

Existing research on blockchain systems frequently evaluates performance in terms of verification speed, operational efficiency, transparency, security, and usability. Studies consistently report that blockchain-based credential verification systems outperform traditional manual verification approaches in several operational aspects.

Research on educational blockchain systems found that blockchain technology substantially improves verification speed by enabling automated credential validation through immutable ledger records and digital signatures. Traditional credential verification processes often require manual communication between institutions and employers, resulting in delays and increased administrative workload. Blockchain systems reduce these inefficiencies by allowing verifiers to independently validate credentials in near real-time (Ismail et al., 2024).

Usability evaluation has become an important area of research, with studies emphasizing that system usability directly influences technology adoption among students, institutions, and employers. Research indicates that blockchain systems with intuitive interfaces, simplified workflows, and transparent verification procedures achieve higher levels of user acceptance (Alammary et al., 2019).

2.4 Synthesis

The reviewed literature emphasizes that blockchain technology provides a secure and decentralized framework for credential management in education and employment. Studies consistently highlight the effectiveness of consortium-based systems in ensuring controlled participation, transparency, and immutability of records, as well as the importance of role-based access mechanisms involving issuers, holders, and verifiers.

The literature further demonstrates that the integration of hashing algorithms, digital signatures, and Decentralized Identifiers strengthens the security and authenticity of blockchain credentials. Existing studies also reveal that blockchain-based credential systems improve verification processes in terms of speed, efficiency, and usability compared to traditional paper-based or centralized methods.

However, despite the growing number of blockchain-related studies, existing research remains limited in terms of comprehensive prototype evaluation integrating architecture design, decentralized identity management, cryptographic security implementation, and usability assessment within a single educational credential verification platform. This research gap supports the significance of the present study.

3. METHODOLOGY

3.1 Research Design

This study adopts a Design Science Research approach, focusing on the construction and evaluation of a novel artifact—the Consortium DLT System. The artifact is designed to solve the specific problem of trust in academic credentials. The following methods were applied in alignment with the three study objectives:

1. **Design and Development Method:** Using an Agile/Iterative development approach for system construction
2. **Experimental Testing:** To measure prototype performance in terms of verification speed and accuracy
3. **Descriptive Statistics:** Specifically mean scores and percentages, to summarize and interpret quantitative results
4. **Survey Questionnaire:** Using a five-point Likert scale administered to respondents to evaluate system usability in terms of ease of use, speed perception, and trust

3.2 Software Development Methodology

The development utilized the Agile Software Development Methodology with an iterative prototyping approach, selected because of its flexibility, incremental development process, and ability to accommodate continuous refinement of system features throughout the development lifecycle.

The development process was divided into six sprints across approximately thirteen weeks:

- **Sprint 0 (Planning):** Requirements gathering, literature review, system design, technology selection
- **Sprint 1 (Foundation):** Next.js scaffold, base routing, initial implementation of MockBlockchainService
- **Sprint 2 (Core portals):** Holder Dashboard, Issuer Dashboard, DID registration, portfolio submission, credential minting
- **Sprint 3 (Verification & cryptography):** Verifier Portal, HMAC-SHA256 signing routine, cryptographic verification flow, ArtifactViewer
- **Sprint 4 (Evaluation):** Respondent evaluation, data gathering, iterative refinement based on feedback
- **Sprint 5 (Finalization):** Documentation, paper revision, defense preparation

3.3 System Architecture and Implementation

The system was built using a modern web technology stack:

- **Frontend Framework:** Next.js 16 with App Router, React 19, TypeScript 5
- **UI Components:** shadcn/ui with Radix UI primitives, Tailwind CSS v4, class-variance-authority (cva)
- **State Management:** Zustand 5 for application state and ledger management
- **Cryptographic Libraries:** CryptoJS 4.2 for SHA-256 hashing and HMAC-SHA256 digital signatures
- **Persistence:** localStorage for state persistence across browser sessions
- **Backend Configuration:** Firebase (Firestore, Authentication, Cloud Storage)

configured for intended production migration

The system implements a three-role architecture:
Holders (Students):

- Submit portfolios with document attachments
- Receive verifiable credentials
- Forward credentials to verifiers
- Monitor credential status
- Communicate with issuers through in-app messaging

Issuers (Universities):

- Review portfolio submissions
- Approve or reject applications
- Mint verifiable credentials with typed metadata and expiry dates
- Digitally sign credentials using HMAC-SHA256
- Revoke credentials when necessary
- Communicate with holders

Verifiers (Employers):

- Receive forwarded credentials
- Validate hashes and digital signatures
- Verify revocation status
- Inspect attached artifacts
- Record verification decisions (accept/decline)

3.4 Data Gathering Techniques

Data gathering employed multiple techniques:

1. **Document Analysis:** Studying existing credential management systems and processes
2. **Observation:** Direct observation of how users interact with the system
3. **Survey Questionnaire:** The main data-gathering tool, a researcher-constructed questionnaire built around ISO/IEC 25010 quality characteristics

3.5 Evaluation Framework

The system was evaluated using the ISO/IEC 25010:2011 quality model, focusing on five characteristics directly observable in a credentialing prototype:

Characteristic	Sub-characteristics evaluated	Operational Definition
Functional Suitability	Functional completeness, functional correctness	The system performs the credential operations it was designed for, and those operations produce the expected results
Performance Efficiency	Time behaviour	The system responds to user actions and completes credential operations within acceptable response times
Usability	Learnability, operability, user-interface aesthetics	A Holder, Issuer, or Verifier can learn, navigate, and operate the system without external assistance
Reliability	Maturity, recoverability	The system behaves the same way across repeated trials and recovers gracefully from interrupted or invalid operations
Security	Integrity, authenticity, non-repudiation	The system protects credentials from unauthorized alteration, confirms the identity of the issuer, and prevents an issuer from denying a credential it has signed

3.6 Respondents and Sampling

The study used purposive sampling, selecting participants based on how well they match the roles in the system. Thirty respondents were recruited:

Respondent Group	Sample Size	Inclusion Criteria
Holders	15	Currently enrolled student or recent graduate (within the last five years) of a tertiary institution
Issuers	5	Registrar, academic administrator, or faculty member with direct involvement in credential issuance
Verifiers	10	Human-resources officer, recruiter, or admissions personnel with experience in credential validation
Total	**30**	

3.7 Research Instrument

The main data-gathering tool was a researcher-constructed questionnaire with 25 Likert-scale items covering the five ISO/IEC 25010 characteristics. Each characteristic was broken down into three to five declarative statements rated on a five-point Likert scale:

- 5 = Strongly Agree
- 4 = Agree
- 3 = Neutral
- 2 = Disagree
- 1 = Strongly Disagree

The questionnaire was organized into six parts: demographics/role identification, functional suitability, performance efficiency, usability, reliability, and security. Each part ended with an open-ended comment field.

The instrument was reviewed by the capstone adviser and pilot-tested with three respondents (none of whom appeared in the final sample) to identify ambiguous items and establish baseline completion time.

3.8 Statistical Treatment

Responses to each Likert item were tallied, and the weighted mean was computed at three levels: per item, per sub-characteristic, and per overall characteristic.

The formula used was:

$WM = (\Sigma\ fw) \div N$

Where WM is the weighted mean, f is the number of respondents who chose a given response, w is the weight attached to that response (5, 4, 3, 2, or 1), and N is the total number of respondents

Each resulting weighted mean was interpreted against equal-interval ranges:

Weighted Mean	Verbal Interpretation	Qualitative Description
4.21 – 5.00	Strongly Agree	Excellent / Very High
3.41 – 4.20	Agree	Good / High
2.61 – 3.40	Neutral	Fair / Moderate
1.81 – 2.60	Disagree	Poor / Low
1.00 – 1.80	Strongly Disagree	Very Poor / Very Low

3.9 Ethical Considerations

The study was conducted in accordance with the Data Privacy Act of 2012 (Republic Act No. 10173) and principles of informed consent, voluntary participation, and confidentiality. Each respondent received a written informed consent form explaining the purpose of the study, nature of involvement, estimated time commitment, and right to withdraw at any point.

Questionnaire data were handled with strict confidentiality. No personally identifiable information was collected. All academic artifacts and credentials used during testing were fictitious. The dataset was stored in a password-protected file accessible only to the researcher and capstone adviser.

4. RESULTS

4.1 Architectural Requirements and Implementation

The Consortium was designed as a secure, role-based decentralized credential management system leveraging consortium blockchain principles, decentralized identity management, cryptographic security, and immutable ledger technologies. The architecture integrates functional and security requirements into a unified framework ensuring credential authenticity, transparency, integrity, accountability, and tamper resistance throughout the credential lifecycle.

System Architecture:

The proposed architecture follows a layered and consortium-based decentralized design combining role-based application portals, decentralized identity management, cryptographic services, immutable ledger recording, and distributed validator nodes within a permissioned blockchain-inspired environment.

Role-Based Access Control: The system implements a strict three-role trust model with explicitly defined functional boundaries:

- **Holders:** Responsible for submitting portfolios, receiving verifiable credentials, forwarding credentials, monitoring credential status, and communicating with issuers
- **Issuers:** Review portfolio submissions, approve or reject applications, mint verifiable credentials, digitally sign credentials, revoke credentials, and communicate with holders

- **Verifiers:** Receive forwarded credentials, validate hashes and digital signatures, verify revocation status, inspect attached artifacts, and record verification decisions

Credential Lifecycle:

The process begins when a Holder submits an academic portfolio or supporting artifact. Upon submission, the system generates a SHA-256 hash key for the submitted artifact. The Issuer reviews pending submissions and, once approved, generates a verifiable credential digitally signed using cryptographic signing mechanisms. Holders may forward credentials to Verifiers for authentication and validation.

4.2 Security Features

The prototype implements hashing, digital signatures, and decentralized identifiers as the core security mechanisms:

Decentralized Identifiers (DIDs):

Each participant is assigned a unique DID formatted as did:consortium:<hash>. During registration, the system generates a cryptographic key pair. The private key is used for signing transactions and credentials, while the public key is stored in the DID Registry and used for signature verification. The DID Registry maps decentralized identifiers to corresponding public keys, enabling trusted identity verification throughout the system.

Hashing Mechanisms:

The system uses SHA-256 hashing to generate unique digital fingerprints for submitted documents, transaction payloads, and credential data. During portfolio submission, multiple uploaded files are aggregated and processed into a combined hash value (artifactHash), ensuring that any modification to submitted documents can be immediately detected. Ledger transactions contain a dataHash field storing the SHA-256 hash of the transaction payload to preserve integrity.

Digital Signatures:

When an issuer approves a student submission, the system creates a verifiable credential object and digitally signs it using HMAC-SHA256 with the issuer's private key. The signing payload includes the credential ID, issuer DID, holder DID, artifact hash, issuance date, attachments hash, credential type, and expiry date, ensuring all credential metadata is cryptographically bound to the digital signature.

Credential Revocation:

Revoked credential identifiers are stored within a dedicated revocation set managed by the blockchain service layer. During credential verification, the system first checks whether the credential exists within the revoked credentials set before proceeding with signature validation and ledger confirmation.

4.3 Ledger Transaction Coverage and Auditability

The results of the ledger transaction coverage and auditability tests demonstrated that the proposed system successfully recorded all major credential-related transactions without failure. Across eight transaction categories, each of the 10 test trials resulted in successful ledger writes with zero failed transactions and no duplicate hashes.

Action Type	Trials (n)	Successful Writes	Failed Writes	Duplicate Hash	Remarks
DID Registration	10	10	0	No	All registrations produced unique hashes
Portfolio Submission	10	10	0	No	Each submission recorded as distinct entry
Portfolio Rejection	10	10	0	No	All rejections recorded with reason
VC Issuance	10	10	0	No	All credentials appended to ledger
VC Revocation	10	10	0	No	All revocations recorded; credentials fail verification
Credential Forward	10	10	0	No	All forwards recorded with message
Credential Decision	10	10	0	No	All accept/decline decisions recorded
Chat Message	10	10	0	No	All messages recorded as transactions

These findings indicate that the developed system possesses a high degree of reliability and consistency in recording transactions on the distributed ledger. The absence of duplicate hashes confirms that each transaction generated a unique cryptographic identifier, ensuring data uniqueness and traceability.

4.4 Portfolio Tampering and Hash Integrity

The portfolio tampering and hash integrity tests evaluated the system's ability to detect unauthorized modifications to submitted portfolio documents. Five tampering scenarios were tested, and in all cases, the modified files generated different hashes from the original versions, resulting in invalid verification outcomes.

Test ID	Modification	Original Hash	Modified Hash	Verification Result	Remarks
T1	Single character edit in PDF	H1	H2	Invalid	Hash changed completely
T2	Metadata alteration	H3	H4	Invalid	Avalanche effect confirmed
T3	File replacement	H5	H6	Invalid	Aggregate hash detects changes
T4	Reordered document set	H7	H8	Invalid	Order-sensitive hashing
T5	Image content modification	H9	H10	Invalid	Binary data integrity preserved

These results confirm the effectiveness of the cryptographic hashing mechanism employed by the system. Even minimal changes, such as altering a single character or modifying file metadata, produced entirely different hash values, demonstrating the avalanche effect characteristic of secure hash functions.

4.5 Credential Revocation

The credential revocation tests assessed whether the system could properly invalidate credentials while preserving the validity of unaffected credentials. The results showed that a valid credential became immediately invalid after revocation and remained invalid during subsequent verification attempts. Non-revoked credentials continued to verify successfully, while revocation attempts by non-issuers were rejected.

Test ID	Action	Pre-Revocation Verify	Post-Revocation Verify	Remarks
R1	Revoke valid credential	Verified	Invalid (Revoked)	Immediate rejection
R2	Re-verify revoked credential	N/A	Invalid (Revoked)	Consistently rejected
R3	Verify non-revoked credential	Verified	Verified	Unaffected by other revocations
R4	Revoke by non-issuer	Verified	Verified (unchanged)	Only original issuer can revoke
R5	Revoke already-revoked	Invalid	Invalid	Idempotent operation

These findings demonstrate that the revocation mechanism operates correctly and securely. Immediate invalidation of revoked credentials prevents continued use of credentials that are no longer valid, thereby enhancing trust among relying parties.

4.6 Verification Speed

The verification speed tests evaluated the efficiency of credential validation under varying document and attachment loads. Results showed verification times of less than 50 milliseconds for a single document, less than 100 milliseconds for three documents, less than 150 milliseconds for five documents with two attachments, and less than 200 milliseconds for five documents with five attachments. Tampered credentials were detected in less than 50 milliseconds, while revoked credentials were rejected in less than 10 milliseconds.

Test ID	Documents	Attachments	Verification Time	Result
V1	1 document	0	<50ms	Verified
V2	3 documents	0	<100ms	Verified
V3	5 documents	2 attachments	<150ms	Verified
V4	5 documents	5 attachments	<200ms	Verified
V5	Tampered credential	0	<50ms	Invalid
V6	Revoked credential	0	<10ms	Invalid (Revoked)

These results indicate that the system maintains excellent performance even as the amount of credential-related data increases. The relatively small increase in verification time as document complexity grows suggests that the verification mechanism scales efficiently.

4.7 Usability Evaluation

The usability survey involved thirty respondents who evaluated the system based on ease of use, speed perception, and trust. The system received a mean score of 4.4 for ease of use, 4.6 for speed perception, and 4.5 for trust, resulting in an overall mean score of 4.5 out of 5.0. All dimensions were interpreted as "Strongly Agree."

Usability Dimension	No. of Respondents	Mean Score (out of 5.0)	Interpretation
Ease of Use	30	4.4	Strongly Agree
Speed Perception	30	4.6	Strongly Agree
Trust in System	30	4.5	Strongly Agree
Overall Mean	**30**	**4.5**	**Strongly Agree**

These findings indicate a high level of user acceptance and satisfaction with the developed prototype. The strong rating for ease of use suggests that users found the interface intuitive and accessible. The highest rating, speed perception, aligns with the objective performance results obtained during verification testing.

4.8 Comparison with Traditional Methods

The comparison between the developed prototype and traditional verification methods highlights substantial improvements in efficiency, security, and reliability. The prototype achieved credential verification in less than 200 milliseconds, whereas traditional verification typically requires 5 to 10 business days due to manual processing and institutional coordination.

Metric	Prototype (Blockchain)	Traditional Method	Remarks
Verification Time	<200 milliseconds	5–10 business days	Significant improvement; near-instantaneous vs. days-long wait
Human Intermediary Required	None	Yes (registrar/admin)	Prototype eliminates administrative bottleneck
Verification Success Rate	100%	Variable (subject to human error)	Prototype provides deterministic, error-free outcomes
Tampered Credential Detection	Automatic (cryptographic)	Manual (may be missed)	100% tamper detection rate vs. unreliable manual review

The prototype achieved a 100% verification success rate and a 100% tampered credential detection rate through automated cryptographic verification. In contrast, traditional methods depend on manual review processes that are susceptible to human error and may fail to detect document alterations.

4.9 Summary of Evaluation Results

The results collectively demonstrate that the developed prototype successfully achieved its intended objectives of providing secure, tamper-resistant, auditable, and efficient credential management. The proposed system exhibited:

- 100% successful transaction recording across all eight transaction types
- 100% tamper detection capability through SHA-256 hashing
- Secure credential revocation functionality with immediate invalidation
- Sub-200 millisecond verification performance
- High user acceptance with an overall usability rating of 4.5/5.0

These findings provide strong evidence that the proposed system is a viable and effective alternative to traditional credential verification approaches, offering significant improvements in security, transparency, efficiency, and user trust.

5. DISCUSSION

5.1 Architectural Design Implications

The successful implementation of the consortium-based distributed ledger architecture confirms that this design approach effectively addresses the limitations of traditional centralized credential management systems. The three-role model (Holders, Issuers, and Verifiers) successfully enforced role-based access control without reliance on trusted third parties or centralized administrators.

The finding that all eight transaction types were recorded with 100% success and no duplicate hashes demonstrates the reliability of the ledger infrastructure. This aligns with previous research by Ismail *et al.*,(2024) and Kumar *et al.*,(2024), who identified consortium blockchain models as highly appropriate for academic environments due to their improved efficiency, controlled access, and institutional accountability.

The system's ability to eliminate single points of failure and prevent unilateral modification of academic records addresses a critical vulnerability identified in the literature. As noted by Sharples and Domingue (2016), immutable ledger structures improve transparency and reduce opportunities for academic fraud. The Ledger Explorer's provision of transparent, filterable access to the complete audit trail further strengthens this capability.

5.2 Security Feature Effectiveness

The combined implementation of SHA-256 cryptographic hashing, HMAC-SHA256 digital signatures, and Decentralized Identifiers proved sufficient to ensure credential integrity, authenticity, and user-controlled management. The portfolio tampering tests confirmed that any modification to submitted documents—even single-character edits or metadata alterations—produced entirely different hash values, demonstrating the avalanche effect characteristic of secure hash functions.

These findings align with research by Tariq *et al.*,(2024), who demonstrated that SHA-256 hashing effectively protects digital credentials from unauthorized modification. The detection of file replacements, reordered document sets, and modified image contents further indicates that the system protects not only textual content but also document structure and binary data integrity.

The digital signature implementation, which cryptographically binds credentials to their issuing institutions through HMAC-SHA256, establishes authenticity and non-repudiation. The extended signing payload—including credential type, metadata, expiry date, and issuer attachments hash—ensures that all credential attributes are immutably bound to the cryptographic proof. This addresses the authentication and integrity verification requirements identified by Ismail *et al.*,(2024) and Naik and Jenkins (2020).

Importantly, by binding credentials to Holder DIDs rather than institution-managed identifiers, the system ensures that students retain permanent ownership of their academic records. This supports the self-sovereign identity principles emphasized in the literature, where individuals maintain ownership and control over their digital identities without dependence on centralized authorities.

The credential revocation mechanism, which immediately invalidates revoked credentials and prevents their continued use, closes a critical security gap identified in traditional systems. The finding that only the original issuer can revoke credentials supports proper governance and prevents unauthorized modifications to credential status, consistent with best practices documented in the literature.

5.3 Performance and Usability Advantages

The substantial improvement in verification speed—from 5-10 business days traditionally to under 200 milliseconds with the prototype—represents a transformative advancement in credential verification efficiency. This finding is consistent with previous research demonstrating that blockchain systems reduce verification delays and minimize manual procedures (Ismail et al., 2024).

The system's scalability is evidenced by the relatively small increase in verification time as document complexity grows (from <50ms for a single document to <200ms for five documents with five attachments). This suggests that the verification mechanism scales efficiently and is suitable for real-world deployment scenarios where fast credential verification is required.

The high usability scores (4.4 for ease of use, 4.6 for speed perception, 4.5 for trust) indicate strong user acceptance, contradicting concerns that blockchain systems present usability challenges for non-technical users (Alammary et al., 2019). The intuitive interface, simplified workflows, and transparent verification procedures contributed to this positive reception.

The 100% verification success rate and 100% tampered credential detection rate represent significant improvements over traditional methods, which are subject to human error and may fail to detect document alterations. The deterministic, error-free outcomes provided by cryptographic verification establish a higher standard of trust and reliability.

5.4 Comparison with Existing Literature

The findings of this study corroborate and extend the existing body of research on blockchain-based credential systems. The successful implementation of a consortium architecture with role-based access control aligns with the recommendations of Alammary *et al.*,(2019) and Ismail *et al.*,(2024). The integration of SHA-256 hashing, HMAC-SHA256 digital signatures, and DIDs reflects the layered security architecture advocated by Naik and Jenkins (2020) and Tariq *et al.*,(2024).

However, this study contributes to the literature by providing comprehensive prototype evaluation integrating architecture design, decentralized identity management, cryptographic security implementation, and usability assessment within a single educational credential verification platform. This addresses the research gap identified in the literature review, where many studies focused on theoretical frameworks or isolated system components rather than complete role-based blockchain credential ecosystems.

The study also provides empirical evidence of the practical benefits of DLT-based credential systems in the Philippine education sector context, where credential fraud and administrative inefficiency have been identified as systemic risks by the Commission on Higher Education.

6. CONCLUSION

6.1 Summary of Findings

This study successfully designed, developed, and evaluated "The Consortium," a prototype DLT-based credential management system for education and employment. The findings demonstrate that:

1. **Architectural Design:**

A consortium-based distributed ledger architecture with a three-role model (Holders, Issuers, and Verifiers) is a viable and effective design for secure credential issuance and verification. The system successfully recorded all credential lifecycle events as immutable ledger transactions, eliminating single points of failure and preventing unilateral modification of academic records.

2. **Security Features:**

The combined implementation of SHA-256 cryptographic hashing, HMAC-SHA256 digital signatures, and Decentralized Identifiers is sufficient to ensure credential integrity, authenticity, and user-controlled management. The system achieved 100% tamper detection capability and secure credential revocation functionality.

3. **Performance and Acceptability:**

The developed prototype significantly improves credential verification over traditional manual methods, achieving verification in under 200 milliseconds compared to 5-10 business days. Usability testing yielded high acceptance scores (overall mean 4.5/5.0), reflecting strong user satisfaction across ease of use, speed perception, and trust.

6.2 Contributions to Knowledge

This study contributes to the body of knowledge on blockchain-based credential systems in several ways:

1. **Comprehensive Prototype Evaluation:** The study provides a complete implementation and evaluation of a role-based blockchain credential ecosystem, addressing the research gap identified in the literature where many studies focused on theoretical frameworks or isolated components.
2. **Contextual Application:** The study demonstrates the applicability of blockchain-based credential systems within the Philippine education sector,

providing a foundation for future production-level implementations.

3. **Practical Implementation Framework:** The system architecture and implementation approach offer a practical model for other educational and employment institutions seeking to participate in a shared, tamper-resistant credentialing network.

6.3 Limitations

This study has several limitations:

1. **Mock Blockchain Service:** The system uses a local simulation of ledger logic rather than a live deployment on a public mainnet, which limits the generalizability of performance results to actual blockchain environments.
2. **Limited Sample Size:** The respondent sample of thirty participants, while adequate for a prototype evaluation, is modest and may not fully represent the diversity of potential users.
3. **No Integration with Legacy Systems:** The system does not integrate with existing university databases, which would be necessary for production deployment.
4. **Local Storage Persistence:** The current implementation uses localStorage for state persistence, which is suitable for prototyping but not production-grade.

6.4 Recommendations

Based on the findings and limitations of this study, the following recommendations are offered:

1. **Controlled Deployment on a Permissioned Test Network:** Future development should transition the mock blockchain service to a controlled, permissioned blockchain test environment such as Hyperledger Besu or a private Ethereum-based test network to validate multi-node consensus, fault tolerance, and inter-institutional governance under simulated real-world conditions.
2. **Migration of Core Logic to Smart Contracts:** Credential issuance, revocation, and verification logic should be migrated into formal smart contracts to ensure on-chain enforcement of critical functions.
3. **Integration with Institutional Record Systems:** Future iterations should integrate the credentialing system with existing university record systems using secure, read-only application programming interfaces (APIs).
4. **Development of a Dedicated Mobile Credential Wallet:** A lightweight mobile credential wallet should be developed to improve usability and accessibility for students, supporting secure storage, selective sharing, offline access, and push notifications.
5. **Incremental Implementation of Privacy-Enhancing Techniques:** Privacy-enhancing mechanisms such as selective disclosure and zero-knowledge proof frameworks should be explored in controlled pilot implementations, starting with simple use cases.
6. **Production Migration to Firebase Backend:** The localStorage-based persistence should be migrated to the already-configured Firebase backend to enable multi-device access, real-time synchronization, and production-grade data durability.

These recommendations emphasize incremental, testable, and governance-aware extensions of the proposed system, supporting responsible adoption of decentralized credentialing technologies within higher education environments.

REFERENCES

- Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences, 9*(12), 2400. https://doi.org/10.3390/app9122400
- Androulaki, E., Barger, A., Bortnikov, V., *et al.*,(2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*. https://doi.org/10.1145/3190508.3190538
- Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments, 5*(1), 1-10.
- Commission on Higher Education. (2020). *ASEAN Plus Three Guidelines on Student Exchanges*.
- Ismail, A., Kumar, R., & Singh, P. (2024). Blockchain-based credential verification

systems: A comprehensive review. *Journal of Educational Technology Systems*, *52*(3), 245-268.

- Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional, 19*(4), 68-72.
- Kumar, S., Sharma, R., & Gupta, A. (2024). Consortium blockchain framework for educational credential verification. *International Journal of Educational Technology in Higher Education, 21*(1), 15-32.
- Merlec, M. M., *et al.*,(2022). A consortium blockchain-based secure and trusted electronic portfolio management scheme. *PubMed Central*.
- Mühle, A., *et al.*,(2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80-286.
- Naik, N., & Jenkins, P. (2020). Decentralized identifiers for self-sovereign identity. *IEEE International Conference on Blockchain and Cryptocurrency*.
- Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. *Proceedings of the 11th European Conference on Technology Enhanced Learning*.
- Tariq, S., Ahmed, M., & Khan, N. (2024). Cryptographic security mechanisms in blockchain credential systems. *Journal of Information Security and Applications, 78*, 103-125.
- Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access, 6*, 5112-5127.
- Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer.