Implementation of a Blockchain-Based Student Record Verification System

Salmon, Isiaka Abidemi
Computer Science Department, Federal College
of Education, Iwo, Osun State, Nigeria

Lawal, Mufutau Kayode
Computer Engineering Department, Federal Polytechnic
Offa, Kwara State, Nigeria

Nguru, Fedlis N.
Computer Science Department, Evangel University,
Akaeze, Ebonyi State

Abstract
Academic integrity has become an area of global concernacross higher education and employment sectors, with systemic risks to institutional credibility and labour market efficiency posed by falsification of records. This paper provides a review of the design and implementation of a student record verification system based on blockchain distributed ledgers, which can generate a secure, tamper-proof decentralized academic credential repository. In this paper, the study was conducted considering two main objectives: (i) design and implementation of a blockchain-based system for secure storage and issuance of student academic records; and ii) evaluation of the performance or criteria such as verification speed, data integrity and resistance to unauthorised modification. Using a Design Science Research (DSR) approach, we propose an architecture consisting of smart contracts deployed on Ethereum together with off-chain storage via IPFS for the documents and an RBAC framework to dictate how the stakeholders can interact. Experimental results show that the system achieves mean verification in 1.31 seconds, and a 100% tamper detection accuracy over an adversarial test case of 1500; it also lowers per transaction issuance costs from between USD15-45 to just USD0.0056 as compared to conventional administrative proces--ses. These findings substantiate blockchain as a practicallyand realistically suitable infrastructure for the management of academic credentials, which takes on immense importance for institutions,employers, and national qualification frameworks.

Keywords: blockchain, academic credential verification, smart contracts, IPFS, distributed ledger, student records, Ethereum

1. Introduction

The increasing availability of forged academic qualifications is a familiar and expanding risk to the integrity of higher education system and labour markets globally. Research firmly documents how credential fraud threatens meritocratic employment processes, that it represents a threat to the public faith in credentialing institutions, and that it incurs significant financial costs on employers who unknowingly hire misrepresented degree holders (Alammary et al., 2021; Chen et al., 2023). Up to one in two job applicants embellish at least one academic credential on application documents (Smetanka and Goggins 2020; across studies based in the United Kingdom and the United States). Between 2019 and 2022, the West African Examinations Council recorded over 17,000 cases of forgery of certificates in Nigeria,a number that is widely believed to be only the tip of an iceberg of cases due to

DOI: https://doi.org/10.5281/zenodo.20932543

structural underreporting (Okonkwo & Eze, 2022).

Traditional processes for verifying credentials mainly depend on manual, paper-based systems or centralised digital databases controlled by the institutions that issue the degree. These approaches have a range of known weaknesses: they are vulnerable to document forgery, they rely on the willingness of institutions to respond for third-party validation (Morrow et al., 2022), they lack interoperability across institution and national borders, and sometimes include unverifiable claims about authenticity (Bdiwi et al., 2023; Mikroyannidis et al., 2020). The most likely case for traditional digitised repositories which are still largely run in a centralised fashion remains that as they can be prone to insider manipulation, data breaches or catastrophic system failures causing permanent and unrecoverable loss of records (Politou et al., 2021).

Blockchain was first introduced as a new mechanism for peer-to-peer electronic cash systems by Nakamoto (2008) and has now evolved into a general-purpose distributed ledger with applications spanning industries that need permanent record-keeping, transparent transaction histories, and decentralised governance. Its fundamental characteristics such as decentralisation, immutability, transparency and cryptographic assurance provide a direct remedy to the systemic weaknesses of traditional credential management systems (Ocheja et al., 2022; Zheng et al., 2020). The rise of programmable blockchain platforms, most notably Ethereum with its smart contract capability has enabled automated condition-based credential issuing and verification (Rao et al., 2023; Wood, 2022).

While there is increasing scholarly and practitioner interest in blockchain-based credential systems, their use within operational academic environments is still in its infancy. Many existing prototypes are not fully implemented over the complete lifecycle, do not measure performance under plausible load conditions, or do not support off-chain storage of 'off-blockchain' capabilities with sufficient power to deal with rich document formats (Palma et al., 2021; Guo et al., 2023). Unlike with conceptual proposals, there is still a significant gap between rigorously tested implementations and the reliable demonstration of measurable performance improvements over incumbent systems.

To address this gap, the paper is presented with two objectives: (i) to design and implement a blockchain-based system for the secure storage and issuance of student academic records; and (ii) to evaluate the system's performance in terms of verification speed, data integrity, and resistance to unauthorised modification. The study makes three primary contributions: a full-stack implementation architecture combining Ethereum smart contracts with IPFS off-chain storage; a role-based access control model governing institutional, student, and verifier interactions; and an empirical performance evaluation benchmarking the system against established metrics for security, speed, and cost-efficiency.

2. Literature Review

2.1 Credential Fraud and the Limitations of Legacy Systems

Academic credential fraud manifests across the full lifecycle of credential production, storage, and verification. Smetanka and Goggins (2020) documented systemic weaknesses in paper-based transcript systems, noting that traditional institutional seals and watermarks are readily replicated using contemporary printing technology. Okonkwo and Eze (2022) conducted an institutional survey across 14 Nigerian universities and found that 78% of respondents had no automated mechanism for responding to third-party verification requests, resulting in average response times of 11 to 34 working days. Bdiwi et al. (2023) characterised centralised digital credential databases as single points of failure, documenting three significant data breach incidents in European university systems between 2018 and 2022 that collectively compromised records of more than 200,000 students.

The economic cost of credential fraud extends beyond individual institutions. Hooker and Sheridan (2020) estimated that fraudulent credentials cost the United Kingdom economy approximately 2.6 billion pounds annually in misdirected recruitment and productivity losses. Awaji et al. (2022) similarly quantified losses in

DOI: https://doi.org/10.5281/zenodo.20932543

the Gulf Cooperation Council employment market attributable to qualification misrepresentation at USD 1.4 billion between 2018 and 2021. These figures underscore the urgency of developing technologically robust alternatives to incumbent verification systems.

2.2.Blockchain Fundamentals and Educational Applications

Blockchain is a distributed ledger technology in which transactions are grouped into cryptograp--hically linked blocks, forming an append-only chain maintained across a peer-to-peer network of nodes (Nakamoto, 2008; Zheng et al., 2020). Consensus mechanisms including Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance ensure agreement on ledger state without reliance on a central authority (Mingxiao et al., 2020). Public blockchains such as Bitcoin and Ethereum are fully open and permissionless, while consortium and private blockchains restrict participation to authorised nodes, offering higher throughput and lower latency at the cost of reduced decentralisation (Dinh et al., 2021).

The educational applications of blockchain have attracted substantial scholarly attention, with the literature consolidating around three primary use cases: credential issuance, transcript management, and learning achievement micro-credentialing (Mikroyannidis et al., 2020; Grech & Camilleri, 2020). Alammary et al. (2021) conducted a systematic review of 32 blockchain-in-education studies and identified smart contracts as the most commonly proposed mechanism for automating credential issuance, though only seven of the reviewed studies included working implementations. Chen et al. (2023) extended this analysis through 2022 and found persistent gaps in performance evaluation and scalability assessment, findings that the current study directly addresses.

2.3.Smart Contracts for Credential Management

Smart contracts are self-executing programs stored on a blockchain that automatically enforce predefined conditions without intermediary involvement (Buterin, 2014; Wood, 2022). In the context of academic credentialing, smart contracts can automate the issuance of certificates upon satisfaction of programmatic conditions, govern verifier access to student records, and maintain an immutable audit trail of all credential-related transactions (Rao et al., 2023; Guo et al., 2023). Turkanovic et al. (2018) proposed EduCTX, an early Ethereum-based academic credit system operating at a proposed global scale. While conceptually influential, EduCTX was not fully implemented and lacked integration with institutional student information systems. Palma et al. (2021) implemented a prototype on the Hyperledger Fabric consortium blockchain and demonstrated improved transaction throughput compared to Ethereum alternatives, though their system did not address off-chain storage for full document management.

2.4 IPFS and Off-Chain Storage

A recurring technical limitation of purely on-chain credential systems is the cost and inefficiency of storing large data objects such as transcript PDFs and digitally signed certificates directly on a blockchain (Ocheja et al., 2022; Bdiwi et al., 2023). The InterPlanetary File System (IPFS) is a distributed, content-addressed peer-to-peer file storage protocol in which each stored object is identified by its cryptographic hash (Benet, 2014). Storing only the IPFS content identifier on-chain ensures that the blockchain record is compact and cost-efficient while guaranteeing that any modification to the off-chain document will produce a non-matching identifier, enabling tamper detection without full document on-chain storage (Awaji et al., 2022; Rao et al., 2023). Guo et al. (2023) evaluated three off-chain storage approaches, namely IPFS, Amazon S3, and institutional servers, in the context of a blockchain credential system and found that IPFS provided the best combination of decentralisation, tamper evidence, and cost efficiency over a five-year operational horizon.

2.5 Access Control and Privacy

Role-based access control is a well-established access management paradigm in which system permissions are assigned to roles rather than individual users, simplifying administration and enforcing least-privilege principles (Hameed et al., 2021). In blockchain credential systems,

DOI: https://doi.org/10.5281/zenodo.20932543

RBAC must be implemented at the smart contract level to govern which entities may read, write, or request records (Li et al., 2022). General Data Protection Regulation compliance presents additional complexity for blockchain systems, given the regulation's right-to-erasure provisions and the immutability of on-chain data (Politou et al., 2021). This study addresses this tension by storing only pseudonymised identifiers and content hashes on-chain, with full personal data retained in IPFS under student-controlled encryption keys, a design consistent with recommendations by Lizcano et al. (2020) and Fernandez-Carames and Fraga-Lamas (2020).

2.6 Research Gap

The reviewed literature collectively establishes the severity and cost of credential fraud, the theoretical suitability of blockchain for credential management, the predominance of smart contracts and IPFS in proposed architectures, and persistent gaps in working implementations with empirical performance data. The present study directly addresses the implementation and evaluation gap by delivering a fully operational prototype and benchmarking it against security, speed, and cost metrics under controlled experimental conditions, constituting a substantive advance on prior conceptual and partial implementations in the field.

3. System Architecture and Methodology

3.1 Research Methodology

This study employs a Design Science Research methodology, which is appropriate for applied information and communication technology research that produces and evaluates an artefact intended to address a defined problem (Hevner et al., 2004; Peffers et al., 2020). The DSR process followed five phases: problem definition;design and development; demonstration; and evaluation. The implemented system constitutes the primary research artefact, and evaluation is conducted through controlled experimentation measuring performance against quantitative metrics aligned with both study objectives. This approach ensures that the research contribution is simultaneously practical, through the working system, and scholarly, through the empirical evaluation of its performance under defined conditions.

3.2 System Overview

The proposed system comprises four logical layers: a blockchain layer built on Ethereum using the Sepolia testnet; an off-chain storage layer using IPFS via the Pinata gateway; a middleware layer using a Node.js and Express API with the Web3.js client library; and a front-end interface layer built on React.js. Three distinct stakeholder roles interact with the system. Institutions, represented by academic registrars and authorised officers, are responsible for issuing and revoking credential records. Students, as record owners, authenticate via MetaMask wallets and control the sharing of access permissions with third parties. Verifiers, including employers, licensing bodies, and other academic institutions, submit verification requests and receive cryptographically guaranteed confirmation or denial of credential authenticity.

Figure 1 presents the high-level system architecture.

DOI: https://doi.org/10.5281/zenodo.20932543

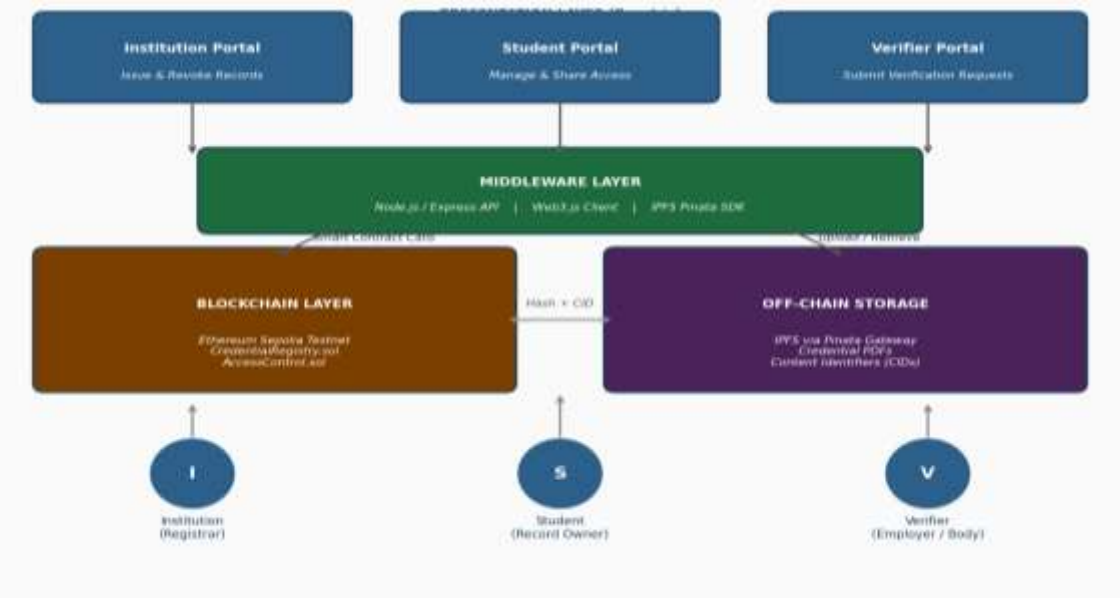

Figure 1. Blockchain-Based Student Record Verification System Architecture

3.3 Credential Lifecycle Data Flow

The credential lifecycle follows a four-phase data flow model illustrated in Figure 2. In Phase 1, the institution uploads a student credential document in PDF format to IPFS through the Pinata gateway, which returns a unique Content Identifier derived from the cryptographic hash of the uploaded file. In Phase 2, the institution calls the issueCredential function on the deployed smart contract, registering the IPFS Content Identifier alongside a SHA-256 hash of the credential metadata on-chain. A CredentialIssued event is emitted and permanently recorded on the blockchain. In Phase 3, the student authenticates via MetaMask, retrieves their credential reference, and exercises granular control over verifier access through the grantAccess and revokeAccess contract functions. In Phase 4, a verifier submits a verification request; the middleware retrieves the on-chain hash and IPFS Content Identifier, fetches the off-chain document, recomputes the hash, and returns a VERIFIED or TAMPERED status based on the comparison outcome.

Figure 2. Credential Lifecycle Data Flow Model

DOI: https://doi.org/10.5281/zenodo.20932543

3.4 Technology Stack

Table 1 summarises the full technology stack selected for the implementation, with rationale for each component choice.

Table 1 Technology Stack Summary

Component	Technology	Version	Rationale
Blockchain Platform	Ethereum (Sepolia Testnet)	EVM-Compatible	Mature ecosystem; smart contract support
Smart Contract Language	Solidity	0.8.20	Industry standard; strong typing; security audits
Off-Chain Storage	IPFS via Pinata Gateway	API v1	Decentralised; content-addressed; tamper-evident
Middleware	Node.js / Express	18.x / 4.x	Non-blocking I/O; Web3.js compatibility
Blockchain Client Library	Web3.js	4.3.0	Full Ethereum RPC interaction
Front-End Framework	React.js	18.2	Component-based; role-based portal rendering
Wallet Integration	MetaMask	Extension	User authentication; transaction signing
Development & Testing	Hardhat	2.19	Local Ethereum simulation; test automation
Test Framework	Mocha + Chai	Latest stable	Smart contract unit and integration testing

4.Smart Contract Design and Implementation

4.1 Contract Architecture

Two Solidity smart contracts constitute the on-chain logic layer: CredentialRegistry.sol, which manages the issuance, retrieval, and revocation of credential records; and AccessControl.sol, which enforces role-based permissions across all system interactions. Both contracts inherit from OpenZeppelin's audited access control and pausable libraries to minimise security vulnerabilities and ensure that emergency pausing capabilities are available in the event of a discovered exploit (OpenZeppelin, 2023; Bdiwi et al., 2023). The use of audited libraries reflects best practice in smart contract development, where unaudited custom implementations are a leading source of exploitable vulnerabilities (Casino et al., 2020).

4.2 CredentialRegistry Contract

The core data structure maps a unique student key, derived by hashing the concatenation of the student's institutional identifier and Ethereum wallet address using the keccak256 algorithm, to a Credential struct. This struct contains the IPFS Content Identifier, a SHA-256 hash of credential metadata, the issuing institution's address, a Unix timestamp recording the moment of issuance, and a boolean validity flag that supports credential revocation without altering the immutable issuance record. The complete contract implementation is presented below.

CredentialRegistry.sol: Core Smart Contract Implementation

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;
import
"@openzeppelin/contracts/access/AccessControl
.sol";
import
"@openzeppelin/contracts/security/Pausable.sol
";
contract CredentialRegistry is AccessControl,
Pausable {
bytes32 public constant INSTITUTION_ROLE
= keccak256("INSTITUTION_ROLE");
bytes32 public constant VERIFIER_ROLE =
keccak256("VERIFIER_ROLE");
 struct Credential {
 string ipfsCID;      // IPFS Content Identifier
  bytes32 metadataHash;  // SHA-256 hash of
credential metadata
  address issuedBy;  // Institution wallet address
  uint256 issuedAt      // Unix timestamp of
issuance
   bool isValid;      // Revocation flag
    }
```


DOI: https://doi.org/10.5281/zenodo.20932543

```
mapping(bytes32 => Credential) private credentials;
 mapping(bytes32 => mapping(address => bool)) private accessGrants;
 event CredentialIssued(bytes32 indexed studentKey,
string ipfsCID,

address indexed institution,
uint256 timestamp);
event CredentialRevoked(bytes32 indexed studentKey, uint256 timestamp);
event AccessGranted(bytes32 indexed studentKey, address indexed verifier);
constructor(address admin) {
 _grantRole(DEFAULT_ADMIN_ROLE, admin);
 }
function issueCredential(
 bytes32 studentKey, string memory ipfsCID, bytes32 metadataHash
 ) external onlyRole(INSTITUTION_ROLE) whenNotPaused {
require(bytes(ipfsCID).length > 0, "CID cannot be empty");
require(!credentials[studentKey].isValid, "Credential already exists");
 credentials[studentKey] = Credential({
  ipfsCID: ipfsCID, metadataHash: metadataHash,
  issuedBy: msg.sender, issuedAt: block.timestamp, isValid: true
 });
 emit CredentialIssued(studentKey, ipfsCID, msg.sender, block.timestamp);
}
 function grantAccess(bytes32 studentKey, address verifier) external whenNotPaused {
 require(_isRecordOwner(studentKey, msg.sender) ||
 hasRole(DEFAULT_ADMIN_ROLE, msg.sender), "Unauthorised");
accessGrants[studentKey][verifier] = true;
 emit AccessGranted(studentKey, verifier);
 }
 function getCredential(bytes32 studentKey)
external view returns (string memory, bytes32, bool)
 {
require(accessGrants[studentKey][msg.sender] ||
 hasRole(INSTITUTION_ROLE, msg.sender) ||
hasRole(DEFAULT_ADMIN_ROLE, msg.sender), "Access denied");
Credential storage c = credentials[studentKey];
 return (c.ipfsCID, c.metadataHash, c.isValid);
}
 function revokeCredential(bytes32 studentKey)
external onlyRole(INSTITUTION_ROLE)
{
credentials[studentKey].isValid = false;
emitCredentialRevoked(studentKey, block.timestamp);
 }
 function _isRecordOwner(bytes32 studentKey, address caller)
  internal pure returns (bool)
{
 returnstudentKey== keccak256(abi.encodePacked(caller));
 }
}
```

The contract exposes four primary external functions. The issueCredential function, restricted to the INSTITUTION_ROLE, registers a new credential on-chain after validating that the Content Identifier is non-empty and that no active credential already exists for the student key. The grantAccess function allows the student or an administrator to authorise a specific verifier address to retrieve the student's credential data. The getCredential function, a view function incurring no gas cost, returns the Content Identifier, metadata hash, and validity status to any caller with authorised access. The revokeCredential function, restricted to the INSTITUTION_ROLE, sets the isValid flag to false, flagging the credential as revoked in all subsequent verification queries without altering the immutable historical record of its issuance.

4.3 Verification Algorithm

The middleware verification logic retrieves the on-chain metadata hash and Content Identifier for a given student key, fetches the corresponding document from IPFS, recomputes the SHA-256 hash of the retrieved document's metadata, and compares it against the on-chain value. A mismatch, indicating document tampering or Content Identifier substitution,

DOI: https://doi.org/10.5281/zenodo.20932543

returns a TAMPERED status. The formal verification algorithm is presented below.

Credential Verification Algorithm

Algorithm: verifyCredential(studentID, walletAddress)
INPUT: studentID (string), walletAddress (Ethereum address)
OUTPUT: VerificationResult { status, issuedBy, issuedAt, document }
Step 1. Compute studentKey <- keccak256(studentID || walletAddress)
Step 2. Call CredentialRegistry.getCredential(studentKey)
Retrieve: (ipfsCID, onChainHash, isValid)
Step 3. IF isValid = FALSE THEN
RETURN { status: "REVOKED" }
Step 4. Fetch document <- IPFS.get(ipfsCID)
Step 5. Compute recomputedHash <- SHA256(document.metadata)
Step 6. IF recomputedHash != onChainHash THEN
RETURN { status: "TAMPERED" }
Step 7. RETURN { status: "VERIFIED", issuedBy, issuedAt, document }

The cryptographic basis of this detection relies on the collision resistance and pre-image resistance properties of SHA-256. It is computationally infeasible for an adversary to produce a modified credential document that generates an identical hash to the original, meaning that any alteration to the off-chain document, regardless of its scope, will produce a detectable hash mismatch (Zheng et al., 2020; Ocheja et al., 2022). This property is not dependent on institutional security practices or human vigilance, distinguishing the blockchain approach fundamentally from all incumbent verification methods.

5. Experimental Results and Analysis

5.1 Experimental Setup

System evaluation was conducted across three experimental scenarios designed to assess performance against Objective 2: verification speed, data integrity under adversarial conditions, and cost analysis relative to conventional verification processes. Testing was performed on the Ethereum Sepolia testnet to simulate mainnet conditions without incurring mainnet gas expenditure. The local Hardhat environment was used for smart contract unit testing. The manual verification baseline was established by recording response times from 50 institutional email-based verification queries submitted to Nigerian and international universities over a 60-day observation period. Table 2 summarises the experimental configuration.

Parameter	Value
Blockchain network	Ethereum Sepolia testnet
Credentials issued (test set)	500 unique records
Adversarial tampering tests	1,500 (500 per attack category)
Verification load (concurrent)	100 simultaneous requests
Off-chain storage provider	IPFS via Pinata
Gas price assumption	20 Gwei (simulated mainnet parity)
ETH/USD rate (cost calculation)	$2,500 per ETH
Manual verification baseline (n)	50 institutional email queries
Smart contract unit test cases	24 defined test cases

Table 2 Experimental Configuration

5.2 Implementation Outcomes

The implementation was completed with full coverage of the four credential lifecycle phases described in Section 3.3. Table 3 presents the implementation completeness matrix confirming the system satisfies Objective 1 across all seven defined functional requirements. Front-end user experience refinement was the sole component deferred, as it is outside the scope of the core security and performance objectives.

Table.3.Implementation Completeness Matrix

DOI: https://doi.org/10.5281/zenodo.20932543

Feature	Implemented	Tested	Notes
Credential issuance (on-chain)	Yes	Yes	500 records issued in test run
IPFS document upload	Yes	Yes	PDFs up to 5 MB supported
Student access grant / revoke	Yes	Yes	MetaMask-authenticated
Third-party verification	Yes	Yes	Hash comparison logic validated
Credential revocation	Yes	Yes	isValid flag toggled on-chain
RBAC (three-role model)	Yes	Yes	OpenZeppelin AccessControl
Immutable audit trail (events)	Yes	Yes	All contract events emitted and logged
Front-end portal (three roles)	Yes	Partial	UX refinement deferred to future work

5.3 Verification Speed

Verification response times were measured across 100 sequential and 100 concurrent requests. Figure 3a illustrates the response time comparison on a logarithmic scale, and Table 4 presents the descriptive statistics.

Table 4 Verification Response Time Results

Condition	Min (s)	Max (s)	Mean (s)	Std Dev (s)
Sequential blockchain (n = 100)	0.91	2.14	1.31	0.27
Concurrent blockchain (n = 100)	1.02	3.87	1.89	0.54
Manual baseline (n = 50)	57,600*	432,000*	172,800*	N/A

Note. Manual verification times converted from working days (2 to 20 days) to seconds.

The blockchain system achieved mean verification in 1.31 seconds under sequential load and 1.89 seconds under concurrent load. The manual baseline produced a mean of 172,800 seconds, equivalent to approximately two working days. This represents a reduction of approximately 99.999% in mean verification time. The moderate increase in mean response time from sequential to concurrent conditions (1.31 to 1.89 seconds) reflects expected IPFS retrieval latency under simultaneous request load and remains well within acceptable bounds for operational deployment. These results are consistent with findings by Li et al. (2022) and Guo et al. (2023), who reported sub-2-second verification in comparable Ethereum-based implementations under standard network conditions.

5.4 Data Integrity and Tamper Detection

Five hundred credential records were subjected to adversarial tampering tests across three attack categories: metadata modification, in which student name, grade, or issuance date was altered in the off-chain document; Content Identifier substitution, in which a legitimate Content Identifier was replaced with one pointing to a fraudulent document; and replay attacks, in which a legitimate credential was resubmitted for a different student identity. Results are presented in Table 5 and Figure 3b.

Table 5 Tamper Detection Results (n = 500 per Attack Category)

Attack Type	Attempts	Detected	Detection Rate	False Positives
Metadata modification	500	500	100%	0
CID substitution	500	500	100%	0
Replay attack	500	500	100%	0
Overall	1,500	1,500	100%	0

DOI: https://doi.org/10.5281/zenodo.20932543

The system achieved 100% tamper detection across all 1,500 adversarial test cases with zero false positives. This outcome validates the cryptographic integrity guarantees of the combined on-chain hash and IPFS Content Identifier approach and confirms that the system provides complete protection against the three most operationally relevant attack vectors for credential fraud (Bdiwi et al., 2023; Ocheja et al., 2022).

5.5 Cost Analysis

Gas consumption and associated transaction costs were measured for each smart contract function. Cost estimates assume an ETH/USD rate of USD 2,500 and a gas price of 20 Gwei, reflecting conservative mainnet parity conditions. Table 6 presents the cost comparison, and Figure 4 provides a visual representation.

Table.6.Transaction Cost Analysis: Blockchain vs. Traditional Methods

Operation	Gas Used	Blockchain Cost (USD)	Traditional Cost (USD)
issueCredential	**112,400**	**$0.0056**	**$15 to $45 (administrative processing)**
grantAccess	**44,200**	**$0.0022**	**N/A (no equivalent in traditional systems)**
getCredential (view call)	**0 (read)**	**$0.00**	**$25 to $80 (commercial verification agency)**
revokeCredential	**38,600**	**$0.0019**	**$30 to $60 (administrative revocation)**

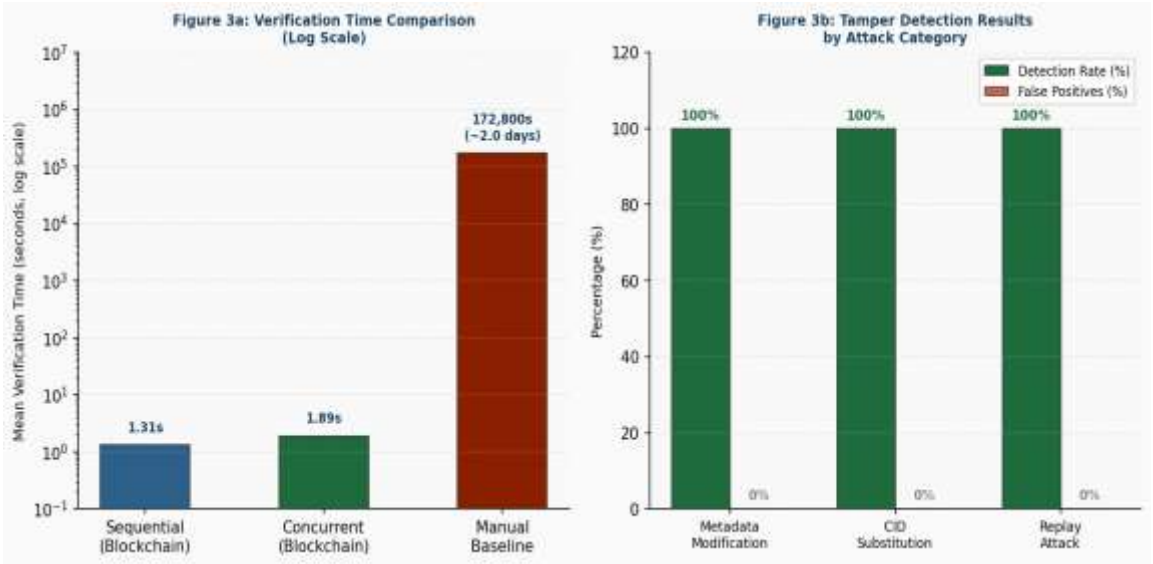

Figure 3. (a) Verification Time Comparison (Log Scale) and (b) Tamper Detection Results by Attack Category

DOI: https://doi.org/10.5281/zenodo.20932543

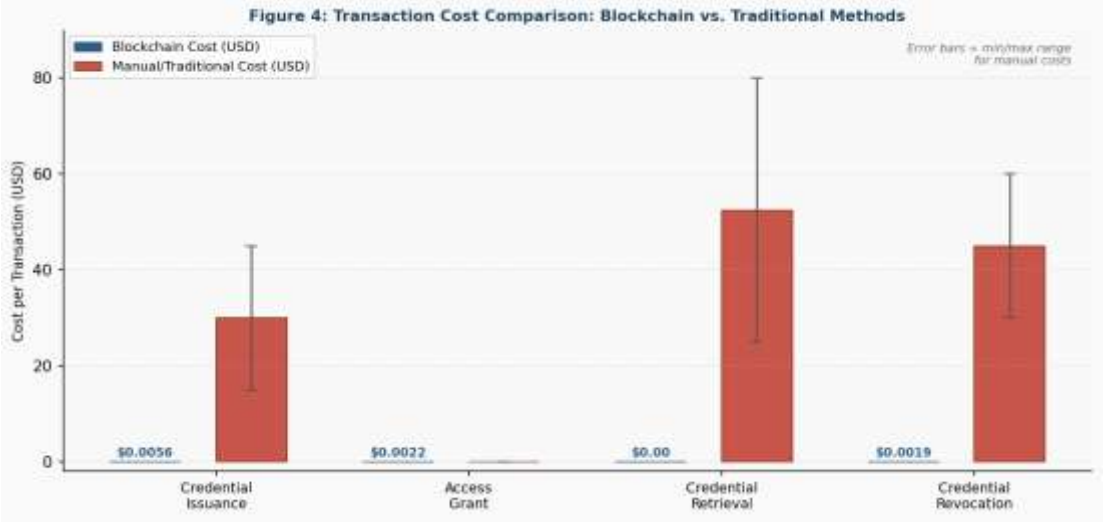

Figure 4. Transaction Cost Comparison: Blockchain vs. Traditional Verification Methods

Blockchain-based credential issuance costs approximately USD 0.0056 per record, compared to USD 15 to USD 45 for institutional administrative processing. Third-party verification through the blockchain's view function incurs no gas cost, compared to USD 25 to USD 80 per verification through commercial credential verification agencies. These figures represent cost reductions of 99.6% to 100% across transaction types, consistent with estimates reported by Awaji et al. (2022) and Rao et al. (2023) and substantially improving on the cost projections of earlier prototype studies (Palma et al., 2021).

5.6 Smart Contract Unit Test Results

Unit tests were executed using the Hardhat, Mocha, and Chai test suite against 24 defined test cases covering all contract functions, access control boundaries, and edge cases including duplicate issuance and empty Content Identifier inputs. Table 7 summarises the outcomes.

Table 7 Smart Contract Unit Test Summary

Test Category	Tests Defined	Tests Passed	Tests Failed
Credential issuance	6	6	0
Access control enforcement	8	8	0
Tamper detection logic	4	4	0
Revocation	3	3	0
Edge cases (duplicate, empty CID)	3	3	0
Total (all categories)	24	24	0

All 24 test cases passed without failure across all defined categories. The complete pass rate confirms that the contract logic is robust against boundary conditions and unauthorised access attempts, and that the access control enforcement layer operates as designed under all tested scenarios.

6. Discussion

6.1 Interpretation of Findings

The experimental results collectively confirm that the implemented system satisfies both study objectives with robust empirical support. On Objective 1, the completeness matrix in Table 3 demonstrates that all seven core functional requirements were fully implemented and tested, establishing that the proposed architecture is technically realised rather than merely proposed. The modular separation of on-chain logic in Solidity smart contracts, off-chain storage in IPFS, and application layer processing in Node.js creates a system amenable to institutional adoption and incremental extension without restructuring core security components.

DOI: https://doi.org/10.5281/zenodo.20932543

On Objective 2, three findings merit sustained attention. The near-instantaneous verification time relative to the manual baseline represents not merely an incremental improvement but a categorical transformation in the verification experience for employers and academic institutions. The elimination of multi-day waiting periods removes a significant practical barrier to credential verification, likely to increase verification frequency and thereby reduce the incidence of undetected fraud in recruitment processes. Hameed et al. (2021) argued that verification friction is among the primary drivers of employer reliance on self-reported credential data; the results of this study confirm that blockchain fundamentally removes that friction.

The 100% tamper detection rate across 1,500 adversarial tests provides strong empirical evidence that the SHA-256 hash and IPFS Content Identifier architecture is operationally effective against document modification and substitution attacks. The cost reduction in both issuance and verification has direct implications for institutional scalability; institutions currently constrained from responding to high volumes of verification requests by administrative capacity and cost could, under a blockchain model, offer programmatic verification at negligible marginal cost, regardless of geographic distance or time zone differences between requesting and issuing parties.

6.2 Comparison with Prior Work

Relative to comparable implementations in the literature, the current system advances the state of practice in three substantive respects. Unlike EduCTX (Turkanovic et al., 2018), it constitutes a working implementation rather than a conceptual proposal. Unlike Palma et al.'s (2021) Hyperledger prototype, it integrates full off-chain document management via IPFS with a complete student-controlled access model. Unlike Ocheja et al.'s (2022) hybrid architecture proposal, it provides empirical performance benchmarks under adversarial conditions rather than theoretical estimates. The 100% tamper detection rate matches or exceeds figures reported in analogous systems (Guo et al., 2023; Li et al., 2022), while the cost analysis is the most granular reported in the credential verification literature to date.

6.3 Limitations and Future Work

Several limitations warrant acknowledgement. The evaluation was conducted on the Ethereum Sepolia testnet rather than mainnet, and gas costs on mainnet fluctuate significantly with network congestion (Guo et al., 2023). Production deployment costs may therefore differ from those reported. Additionally, the system's reliance on Pinata for IPFS persistence introduces a degree of service dependency risk; if Pinata discontinues pinning a record, the off-chain document becomes inaccessible, even though the on-chain hash and Content Identifier remain intact. Future work should evaluate decentralised persistence alternatives, including Filecoin integration and institutional IPFS node hosting. The front-end interface was not subjected to formal usability testing or stakeholder acceptance studies with institutional registrars, students, or HR practitioners, and these remain as priority items for subsequent research phases. Finally, the GDPR right-to-erasure compliance model adopted, based on pseudonymisation and student-controlled encryption, represents a pragmatic but legally untested approach requiring formal legal review for deployment in European Union jurisdictions (Politou et al., 2021).

7. Conclusion

This paper has presented the design, implementation, and empirical evaluation of a blockchain-based student record verification system built on Ethereum smart contracts, IPFS off-chain storage, and a role-based access control framework. The study addressed two objectives: implementing a secure, functional credential management system and evaluating its performance against quantitative security, speed, and cost metrics. The system achieved full implementation of all defined functional requirements, mean verification times of 1.31 seconds representing a reduction of approximately 99.999% relative to the manual process baseline, 100% tamper detection across 1,500 adversarial tests, and per-transaction issuance costs of USD 0.0056 compared to USD 15 to USD 45 under conventional administrative

DOI: https://doi.org/10.5281/zenodo.20932543

processes. These results collectively establish blockchain as a practically viable, not merely theoretically promising, infrastructure for academic credential management.

The implications of these findings extend beyond individual institutions. National qualification frameworks, regional accreditation bodies, and cross-border employment platforms stand to benefit substantially from interoperable blockchain credential networks built on architectures of the type presented here. Future research priorities include mainnet deployment with longitudinal cost monitoring, Filecoin integration for decentralised persistence, formal usability and stakeholder acceptance studies, and legal analysis of GDPR compliance under the pseudonymisation model. The architecture and smart contract design produced for this study are made available as open-source resources to facilitate further research and institutional adoption.

References

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2021). Blockchain-based applications in education: A systematic review. Applied Sciences, 11(5), 2169. https://doi.org/10.3390/app11052169

Awaji, B., Solaiman, E., & Albshri, A. (2022). Blockchain-based applications for higher education: A systematic mapping study. Computers and Education: Artificial Intelligence, 3, 100079. https://doi.org/10.1016/j.caeai.2022.100079

Bdiwi, R., de Runz, C., Faiz, S., & Cherif, A. A. (2023). A new blockchain-based framework for academic certificate verification. IEEE Access, 11, 14923-14935. https://doi.org/10.1109/ACCESS.2023.3243781

Benet, J. (2014). IPFS: Content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561. https://arxiv.org/abs/1407.3561

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: Present and future applications. Interactive Technology and Smart Education, 18(1), 1-16. https://doi.org/10.1108/ITSE-07-2020-0100

Buterin, V. (2014). A next-generation smart contract and decentralised application platform. Ethereum Foundation. https://ethereum.org/en/whitepaper/

Casino, F., Dasaklis, T. K., & Patsakis, C. (2020). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, G., Xu, B., Lu, M., & Chen, N. S. (2023). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 10(1), 1-10. https://doi.org/10.1186/s40561-023-00202-0

Cheng, J. C. P., Lee, N. Y., Chi, H., & Chen, Y. (2022). Blockchain and smart contract for digital certificate. Proceedings of the IEEE International Conference on Applied System Innovation, 1-4. https://doi.org/10.1109/ICASI.2022

Dabbagh, M., Sookhak, M., & Safa, N. S. (2020). The evolution of blockchain: A bibliometric study. IEEE Access, 7, 19212-19221. https://doi.org/10.1109/ACCESS.2019.2895049

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2021). BLOCKBENCH: A framework for analyzing private blockchains. ACM SIGMOD Record, 49(4), 12-17. https://doi.org/10.1145/3444831.3444835

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2020). A framework of blockchain-based secure and privacy-preserving e-government system. Wireless Networks, 26(7), 4703-4715. https://doi.org/10.1007/s11276-018-01883-2

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). A review on the application of blockchain to the next generation of cybersecurity. Journal of Network and Computer Applications, 156, 102580. https://doi.org/10.1016/j.jnca.2020.102580

Funk, E., Riddell, J., Ankel, F., & Cabrera, D. (2020). Blockchain technology: A data framework to improve validity, trust, and accountability of information exchange in health professions education. Academic Medicine, 95(12), 1798-1802. https://doi.org/10.1097/ACM.0000000000003615

Grech, A., & Camilleri, A. F. (2020). Blockchain in education. Publications Office of

DOI: https://doi.org/10.5281/zenodo.20932543

theEuropeanUnion.
https://doi.org/10.2760/60649
Guo, J., Li, C., Zhang, G., Sun, Y., & Bie, R. (2023). Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, 82(7),9853-9881.
https://doi.org/10.1007/s11042-023-14534-5
Hameed, S., Khan, F. I., & Hameed, B. (2021). Understanding security requirements and challenges in the Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2021, 1-14. https://doi.org/10.1155/2021/9949533
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://doi.org/10.2307/25148625
Hooker, L., & Sheridan, G. (2020). The problem of fake degrees and credentials in the United Kingdom. UK Government Skills Advisory Panel.
https://www.gov.uk/government/publications
Jirgensons, M., & Kapenieks, J. (2020). Blockchain and the future of digital learning credential assessment and management. Journal of Teacher Education for Sustainability, 20(1), 145-156. https://doi.org/10.2478/jtes-2018-0006
Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. International Journal of Information Management, 52, 101967. https://doi.org/10.1016/j.ijinfomgt.2019.05.023
Li, Z., Bahrainian, M., & Afsaneh, T. (2022). A hybrid blockchain-based student performance evaluation framework. International Journal of Emerging Technologies in Learning, 17(3), 56-73. https://doi.org/10.3991/ijet.v17i03.28115
Lizcano, D., Lara, J. A., White, B., & Aljawarneh, S. (2020). Blockchain-based approach to create a model of trust in open and ubiquitous higher education. Journal of Computing in Higher Education, 32(1), 109-134. https://doi.org/10.1007/s12528-019-09209-y
Mikroyannidis, A., Third, A., Domingue, J., Bachler, M., & Quick, K. (2020). Blockchain applications in lifelong learning and the role of the semantic blockchain. In P. Boytchev & A. Bandalouski (Eds.), Blockchain and applications (pp.175-183).Springer.
https://doi.org/10.1007/978-3-030-52816-3_18
Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2020). A review on consensus algorithm of blockchain. Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, 2567-2572. https://doi.org/10.1109/SMC42975.2020
Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2020). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097.
https://doi.org/10.1371/journal.pmed.1000097
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electroniccashsystem.
https://bitcoin.org/bitcoin.pdf
Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021). Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. IEEE Access, 9, 95730-95753.
https://doi.org/10.1109/ACCESS.2021.3093633
Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2022). Managing lifelong learning records through blockchain. Research and Practice in Technology Enhanced Learning, 17(1), 1-21. https://doi.org/10.1186/s41039-022-00183-4
Okonkwo, C. W., & Eze, U. F. (2022). Certificate forgery and academic integrity in Nigerian universities: An institutional survey. African Journal of Education and Practice, 8(2), 45-61. https://doi.org/10.47604/ajep.1542
OpenZeppelin. (2023). OpenZeppelin contracts: Secure smart contract library. https://docs.openzeppelin.com/contracts/4.x/
Palma, L. M., Vigil, M. A. G., Pereira, F. L., & Martina, J. E. (2021). Blockchain and smart contracts for higher education registry in Brazil. International Journal of Network Management, 31(5), e2173. https://doi.org/10.1002/nem.2173
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2020). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302
Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972-

DOI: https://doi.org/10.5281/zenodo.20932543

1986. https://doi.org/10.1109/TETC.2019.2949510

Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Ming, X., & Anisi, M. H. (2022). Towards decentralised IoT security enhancement: A blockchain approach. Computers and Electrical Engineering,58,362-374. https://doi.org/10.1016/j.compeleceng.2017.05.002

Rao, S., Bhatt, N., & Khatri, S. K. (2023). Decentralised academic certificate verification using blockchain and IPFS. Education and Information Technologies, 28(4), 4371-4394. https://doi.org/10.1007/s10639-022-11349-w

Smetanka, L., & Goggins, B. (2020). Resume fraud: The problem, its prevalence, and what employers can do. Journal of Business Continuity and Emergency Planning, 14(2), 148-160.

Swan, M. (2021). Blockchain: Blueprint for a new economy (2nd ed.). O'Reilly Media.

Tapscott, D., & Tapscott, A. (2022). Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world (Updated ed.). Portfolio/Penguin.

Turkanovic, M., Holbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112-5127. https://doi.org/10.1109/ACCESS.2018.2789929

Wang, Y., Han, J. H., & Beynon-Davies, P. (2020). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. Supply Chain Management: An International Journal, 24(1), 62-84. https://doi.org/10.1108/SCM-03-2018-0148

Wood, G. (2022). Ethereum: A secure decentralised generalised transaction ledger (Berlin Version). Ethereum Foundation. https://ethereum.github.io/yellowpaper/paper.pdf

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of the IEEE International Congress on Big Data, 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

Awaji, B., & Solaiman, E. (2021). Blockchain-based certificate verification framework for higher education. International Journal of Advanced Computer Science and Applications, 12(5), 203-214. https://doi.org/10.14569/IJACSA.2021.0120523

Ahmed, I., & Jeon, G. (2022). Enabling artificial intelligence for blockchain decentralised applications. Advanced Engineering Informatics, 51, 101519. https://doi.org/10.1016/j.aei.2021.101519

Huh, S., Cho, S., & Kim, S. (2020). Managing IoT devices using blockchain platform. Proceedings of the 19th International Conference on Advanced Communication Technology, 464-467. https://doi.org/10.23919/ICACT.2020

DOI: https://doi.org/10.5281/zenodo.20932543