Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 2, 2026

BLOCKCHAIN-BASED TEMPER-PROOF AND DECENTRALIZED FRAMEWORK FOR EDUCATIONAL DOCUMENTS VERIFICATION

Neha-e-Noor Shaikh[1], Muhammad Hanif Tunio[*2], Ali Nawaz Sanjrani[3], Muzammil Iqbal Shaikh[4], Noor Ahmed Shaikh[5], Asadullah Kehar[6]

[1,*2,5,6]*Institute of Computer Science, Shah Abdul Latif University, Khairpur Sindh-Pakistan*
[3]*Department of Mechanical Engineering, Mehran University of Engineering and Technology, SZAB Campus, Khairpur, Sindh, Pakistan*
[4]*Department of Computer Science, Muhammad Ali Jinnah University, Karachi, Sindh-Pakistan*

[*2]hanif.tunio@salu.edu.pk

DOI: https://doi.org/10.5281/zenodo.18668792

Keywords

Article History
Received: 18 December 2025
Accepted: 02 February 2026
Published: 17 February 2026

Corresponding Author: *
Muhammad Hanif Tunio

Abstract

The fast digitalization of the educational systems has contributed greatly to the demands of secure, reliable, and efficient mechanisms for verifying academic documents. Existing verification systems are centralized, manual, and time-consuming, and hence susceptible to document forgery, data tampering, and inefficiency in operations. To alleviate these issues, this paper presents a Blockchain-Based Tamper-Proof and Decentralized Educational Documents Verification Framework that provides a high level of security, transparency, and trust without any references to a single authoritative organization. The developed framework uses a permissioned blockchain system that has been implemented with cryptographic hashing (SHA-256), cryptography-based digital signatures, and Merkleized block formations to ensure there is integrity and non-mutability of the data. Educational certificates are created in a standardized format of JSON, hashed, signed by authorized institutions, and anchored safely on the blockchain. Confirmation is carried out by re-hashing document hashes and cryptographic signatures with immutable ledger records so that instant and reliable authentication can be done. To simulate realistic academic workloads, an academic system prototype model was developed and tested with synthetic certificate datasets. Several experiments were conducted on changing the key parameters like the batch size, worker parallelism, and certificate tampering rates to determine scalability, performance, and resiliency. Experimental outcomes indicate that it has high issuance throughput (up to 952 transactions per second (TPS)), effective verification performance, low median latency (between 3 and 4 ms), and can detect a tamper (TDR = 100%), and zero false acceptance and false rejection in all test conditions. The results of this research work affirm that blockchain technology, with an effective batching and parallel processing policy, can be used to offer a scalable and secure solution to large-scale examination of educational documents. The study provides a validated framework and empirical evidence that can be used to implement blockchain-based credential verification systems in an academic and institutional setting.

INTRODUCTION

In the present day digital age, students are given degrees and certificates as testimony of their success. However, there is a lot of forging certificates and counterfeiting credentials, and the tampering of academic records. The universal processes to check the validity of

documents rely on a central institution such as a university or a government department, and thus, it is quite expensive, inefficient, slow, and subject to human errors and computer viruses. The systems that are outdated, such as this, are doomed to fail, and therefore, there should be a system of verification that is accurate, decentralized, and at the same time, fast. Reports by the United Nations Educational, Scientific, and Cultural Organization (UNESCO) estimate that the number of forged or manipulated degrees, transcripts, and certificates is in the thousands globally every year and is compromising the integrity of the educational institutions and equity of the professional opportunities [1]. Counterfeit diplomas and forged academic documents have become a significant challenge to the sanctity of the education systems, and the effects of such actions span both the educational and the social and market segments. As an example, employing unqualified people in sensitive areas like medicine, law, or engineering may result in disastrous effects in terms of morality as well as pragmatics [2].

The conventional verification systems are usually centralized and reliant on manual validation by issuing institutions or government departments. Such systems are very time-consuming, expensive and liable to human mistakes and cyber attacks. Furthermore, there are no standardized digital frameworks across institutions and countries, complicating and rendering cross-border verification complex and unreliable. This archaic model is no longer viable in a world that is becoming more digitally transformed and mobile in the global context [3][4]. To address these shortcomings, it is necessary to have an automated, dependable, and non-tamperable verification scheme that guarantees the authenticity and integrity of educational qualifications. In this respect, a revolutionary solution can be offered to blockchain technology, which is a distributed ledger system that is characterized by immutability, transparency, and decentralization. Blockchain also removes intermediaries by enabling them to store information in a distributed network of nodes, which still ensures that when data is stored, it cannot be modified or erased. This aspect renders it appropriate in document verification and record management in the field of education [5-7].

The use of blockchain technology ensures information security by making the system inaccessible to changes and unnecessary, as there is no single authoritative figure that would handle the issue. In connection with its aforementioned concept of distributed ledger technology, blockchain incorporates the safety of the information with the transparency through the use of encrypted data, which is kept in a time-stamped format. Blockchain operates within decentralized networks, which is equivalent to the fact that there are no intermediaries required. This is a significant alleviation of forgery in the documentation. As mentioned above, the framework is not based on a checking authority, i.e., all is done by using smart contracts, which streamlines the whole blockchain verification process because credentials are no longer physically checked [8][9]. Blockchain can assist in verifying educational documents to avoid fraud and increase the level of trust between the two parties, besides simplifying the authentication process for employers, educational institutions, and verification agencies. When students get their certificates, they can put them on the blockchain using a cryptographic signature. Companies that can be interested in authenticating and verifying the document compare it to the hash in the blockchain. It prevents any manipulation of the academic records and allows verifying the records universally, which increases the cross-border credential checking [10-13].

Blockchain refers to a distributed cryptographic registry where transactions are documented in a chain of unchangeable blocks. Block numbers are connected to the former one with the help of cryptographic hashes to create a verifiable chain of records that is secure. In contrast to the conventional databases, blockchain does not have any central authority and instead, every node of the network keeps a copy of the ledger, which ensures decentralization and validation based on consensus. Figure 1. The interlocking blocks in the blockchain, as shown in Figure 2. Displays the layout of the individual block in the blockchain [14-16].

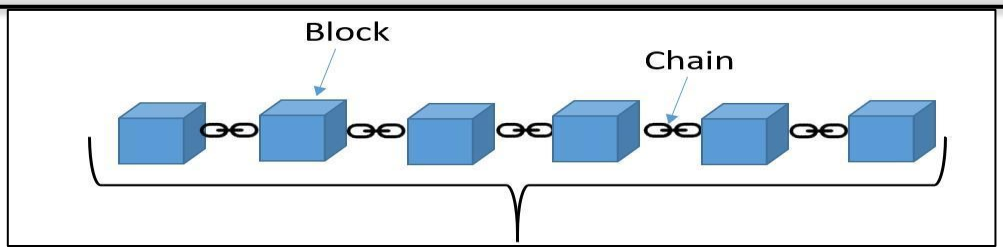

Figure 1 The Longest chain in the blockchain is the accepted chain

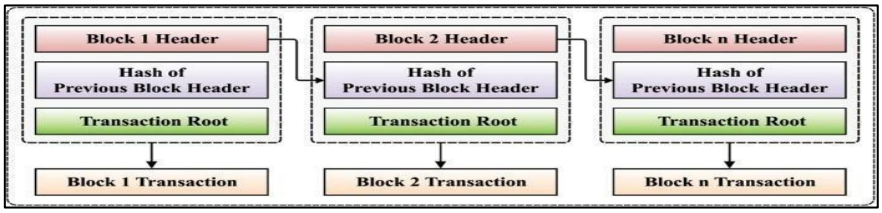

Figure 2 Structure of Blocks in Block Chain

This paper presents the context and the reason behind the creation of a blockchain-based, tamper-proof, and decentralized system of verifying educational documents. It underscored the increasing issue of academic credential fraud, the inefficiencies in conventional centralized verification methods, and the consequent problems to the universities, employers, and most specifically the students, especially in developing economies like Pakistan. As mentioned, the immutability, decentralization, and transparency factors of blockchain technology provide a potential solution to the credibility, integrity, and efficiency of managing academic credentials. The rest of the paper sections present Section 2: Related Work: Surveys on related work in blockchain applications for document verification. Section 3 presents the Research Methodology, which describes Data generation and preprocessing, research design, system architecture, framework development, blockchain logic, and metrics of performance evaluation. Chapter 4 presents Experimental and Simulation Results: Provides testing of experimental results and performance tests. Chapter 5: Conclusion and Future Work provides an overview of the findings and recommends the areas of future research.

2. COMPREHENSIVE REVIEW OF RELATED WORK

2.1 Evolution of Blockchain Technology

The origin of blockchain technology dates back to 2008 when Satoshi Nakamoto presented his work as the backbone of Bitcoin. Originally intended to support decentralized digital money transfer, blockchain has currently been transformed into a platform with multiple uses, being the distributed ledger system that can safely store and authenticate transactions without the involvement of intermediaries [29]. During the first phase, called Blockchain 1.0 the technology mainly delivered the cryptocurrency applications. This iteration was aimed at facilitating a network consensus mechanism to permit peer-to-peer (P2P) financial transactions which eliminated the potential of double-spending as well as centralized authority. With this innovation, the trust issue had been resolved since there were cryptographically linked blocks that tracked irreversible histories of transactions and were held collectively by network nodes [30].

Later developments saw the emergence of Blockchain 2.0, which opened the opportunities of the technology beyond cryptocurrency. It implemented smart contracts, which are self-executing applications that automatically impose the previous conditions of an agreement. This development has made it possible to manage digital assets, records, and business processes with decentralization in various sectors such as finance, supply chain, identity management, and education. Subsequent developments, commonly referred to as Blockchain 3.0, have focused on promoting interoperability, scalability, and energy efficiency in order to facilitate a wider range of adoption in

institutional and government environments [31, 42-43].

2.2 Technical Foundations of Blockchain

A blockchain is a decentralized and distributed electronic registry in which every block includes a register of transactions that are verified and cryptographically connected to the previous block through a hash function. The ledger is a network of participants known as nodes that adhere to a consensus mechanism to decide on the validity of new transactions [29].

2.2.1 Distributed Ledger Structure

The network has redundancy and resiliency because every node contains an identical copy of the ledger. Since the information is duplicated on more than one node, the network identifies any unauthorized changes to an information copy immediately. This decentralization gets rid of the dependence on one authority and increases the integrity of data.

2.2.2 Consensus Mechanisms

Consensus algorithms play a key role in establishing trust in a trustless environment. PoW, PoS, DPoS, and Practical Byzantine Fault Tolerance (PBFT) are the common mechanisms [32].

- **PoW** as used by Bitcoin, is computationally intensive and uses computational power to validate transactions.
- **PoS** is more energy efficient since it replaces the computation with staking of tokens.
- **PBFT** is mostly adopted in permissioned blockchains, which can achieve quicker consensus in a private network, which is ideal for institutional applications, such as education.

2.2.3 Immutability and Transparency

When a transaction has been registered and confirmed, it cannot be changed without unanimity by any of the participants. All transactions are also time-stamped and verifiable with an audit trail of everything that has been done in a blockchain. Such characteristics render blockchain especially useful in those cases when the integrity of data and the absence of the possibility of being mistaken are crucial, including the issuance and checking of educational qualifications[33].

2.2.4 Smart Contracts

Smart contracts are self-executing functions acting as self-executing agreements that process transactions according to specific requirements. A smart contract can be used in credential verification to issue, store and verify certificates through cryptographic hashes, thus removing human intervention. They supplement automation, transparency, and efficiency and minimise mistakes and the cost of operation [34].

2.3 Traditional Academic Document Verification Systems

Historically, the conventional methods of checking academic qualifications were based on centralized and manual academic credential checking. Most universities utilize the paper certificates or hardcopy digital versions that are kept in university databases. Checking of requests is done by post, e-mail or physical verification by employers or other institutions [35].

This strategy has many limitations:

- **Forgery and Tampering:** Paper Certificates are easy to forge or manipulate with the help of digital editing software.
- **Centralized Control:** This reliance on issuing institutions gives a single point of failure and leaves out access to verification services out of office hours and outside geographical boundaries.
- **Time and Cost Inefficiency:** Manual authentication is associated with bureaucracies, and it can take several days and weeks to verify authenticity.
- **Lack of Interoperability:** There is a deficiency of an internationally accepted standardized system of digital credentialing, which prevents cross-border recognition.
- **Security Vulnerabilities:** Central databases are vulnerable to hacking, manipulations by insiders, and data breaches.

Such issues are especially sharp in developing countries, especially in Pakistan, where the level of digitization is low, as well as the inefficiency of the data infrastructure and a lack of coordination between institutions. Thus, employers and universities consume a lot of

time and resources to authenticate credentials, whereas students cannot get a job or be enrolled in international educational institutions..

2.4 Blockchain In Education: Conceptual Frameworks

The most recent studies have discussed that blockchain could reshape the educational ecosystem through the delivery of decentralized, tamper-proof, and verifiable digital records. The core characteristics of blockchain, such as immutability, transparency, and cryptographic security, are relatively compatible with an academic records management system and credentials verification.

2.4.1 Blockchain for Academic Credentials

A credentialing system based on blockchain solutions stores a cryptographic hash of every academic record in the ledger. A digital fingerprint (hash) of a certificate is stored on the blockchain when issued by a student or an institution. When a document is being verified, it is hashed once again, and when the two hashes are equal, then the credential is authenticated to be genuine. This avoids the possibility of forgery and offers instant verification [36].

2.4.2 Decentralized Identity and Ownership

Blockchain enables learners to have self-sovereign identities, i.e. they hold and manage their credentials without the aid of third parties. This kind of a model would foster privacy of the data at the same time facilitating interoperability across institutions and borders [29].

2.4.3 Smart Contracts in Credential Issuance

Smart contracts involve the automation of the lifecycle of credentials, between issuance and validation up to revocation. When a university gives a degree out, the smart contract will automatically document the transaction, inform the concerned parties and offer real-time authentication to the employers [17-20].

2.4.4 Use of Permissioned vs. Public Blockchains

Public blockchains (e.g., Ethereum) are more transparent and open but can be a privacy threat. The permissioned blockchains (e.g., Hyperledger Fabric or Corda) are more appropriate in education as they provide only access to authorized institutions and reflect the transparency versus confidentiality [37].

2.5 Blockchain-Based Verification Systems

An increasing amount of literature has studied blockchain-acquired academic verification solutions:

- **Chen et al. (2018)** suggested a system of educational records management based on blockchain, which guarantees integrity and non-repudiation, but indicated difficulties with interoperability between the institutions [38].
- **Gao and Li (2019)** The decentralized certificate verification model of Gao and Li (2019) employed smart contracts, but their prototype proved to have scalability problems in the case of a high data load [39].
- **Turkanović et al. (2019)** proposed EduCTX, a blockchain-based global platform for hosting of higher education credits, which enables the sharing of student performance in a safe and transparent manner [40].
- **Gräther et al. (2021)** have created a credential management system with Hyperledger Fabric, which gave fine-grained access control and privacy protection but demanded a large infrastructure investment [41].
- **Panda et al. (2022)** analysed the potential of blockchain to verify student transcripts in developing countries and came to the conclusion that a hybrid (public-private) approach could bring a balance between transparency and effectiveness.

Put together, these articles show the potential of blockchain in credential management, but also depict a gap in the validation of empirical support, scalability, and practical application. The majority of frameworks are conceptual or empirical in nature, with small datasets and no comprehensive performance tests in a realistic institutional environment. Table 1 discusses the detailed summary of the reviewed studies.

Table 1. Summary of Reviewed Studies on Blockchain-Based Academic Verification Systems

Reference	Year	Key Issue Addressed	Proposed Approach	Results and Limitations
[21] Saleh et al. Blockchain Based Framework for Educational Certificates Verification	2020	Gaps in existing certificate verification solutions (authenticity, privacy, ownership); need for a secure framework.	Design and propose a Hyperledger Fabric–based framework with Merkle hashing and permissioned channels for secure certificate verification.	Conceptual framework outlining transaction flow; no large-scale empirical evaluation or performance benchmarks.
[22] Grech et al. Blockchain and Higher Education Diplomas (Review / Cases)	2021	Lack of unified and practical blockchain solutions for higher education; fragmented pilot studies.	Systematic review and case studies of projects such as Blockcerts; comparison of cost, scalability, and latency trade-offs.	Summarizes pilot implementations and performance metrics; most studies remain pilot-level with limited reproducibility.
[23] Scientific Reports – Blockchain Ensuring Academic Integrity (Hybrid Prototype)	2025	Real-world prototype for issuance and verification with measurable latencies and functional validation.	Developed a Python and Docker-based hybrid blockchain prototype; implemented QR-based verification with consensus replication.	Measured registration ≈2.97s and signing ≈0.96s; validated feasibility, but scalability beyond moderate loads remains untested.
[24] Abdelmagid et al. A Blockchain Framework for Academic Certificates (IJACSA)	2024	Academic credential fraud and the need for performant permissioned blockchain systems.	Implemented Hyperledger Fabric deployment; analyzed transaction throughput (TPS) against node scalability.	Found Fabric to achieve higher TPS; latency increases with participant count. Limited reproducible large-scale data.
[25] Educational Certificate Verification System (Ethereum + IPFS)	2024	Need for a practical off-chain storage architecture integrating blockchain for certificate verification.	Proposed Ethereum smart contract integrated with IPFS for decentralized off-chain content storage and on-chain hash anchoring.	Demonstrated efficient issuance and IPFS anchoring; noted gas cost challenges and limited privacy handling for metadata.
[26] Rachel et al. Survey: Blockchain for Verification of Academic Certificates (Zenodo)	2023	Overview of state-of-the-art blockchain-based verification frameworks and identification of research gaps.	Surveyed existing models and compared design architectures such as Merkle trees, Blockcerts, and permissioned/permissionless systems.	Highlighted the lack of empirical testing and standard benchmarking; survey-based insights without implementation.
[27] Multiple-Case Study:	2022	Analyzed socio-technical benefits	Conducted multiple-case qualitative analysis linking	Confirmed blockchain improves

Benefits of Blockchain for Digital Certificates (ScienceDirect)		and organizational adoption barriers of blockchain certification systems.	blockchain features to institutional outcomes.	trust and transparency, but identified integration and skills barriers; no quantitative performance data.
[28] Noorhizama et al. Verification of Ph.D. Certificate using QR Code on Ethereum	2023	Focused on a low-cost, practical verification approach using QR code anchors on the Ethereum blockchain.	Developed a prototype issuing QR-enabled certificates with metadata anchored on-chain for instant verification.	Validated user-friendly QR verification, but limited scalability and cost-effectiveness for large-scale deployment.

Even though blockchain technology has remarkable benefits in the aspects of decentralization, immutability, and transparency, it has not been adopted in document verification in educational institutions because various issues related to it have not been addressed. A critical appraisal of the available literature indicates that the majority of the literature is merely general or, more so, lacks systematic and quantitative validation based on realistic academic circumstances.

3. RESEARCH METHODOLOGY

The study has carried out in a research design and implementation-oriented study that is geared towards the creation and testing of a blockchain-based framework of secure and decentralized assurance of educational credentials. The design is based on the Design Science Research (DSR) methodology that focuses on the development of a new artifact to address a real-world issue that is the case, academic credentialing forgery and ineffective verification systems. The new product created is a permissioned prototype of a blockchain that proves how decentralized technologies can make academic records authentic, transparent, and immutable. The flow of the research design of the proposed approach is presented in Figure 2.

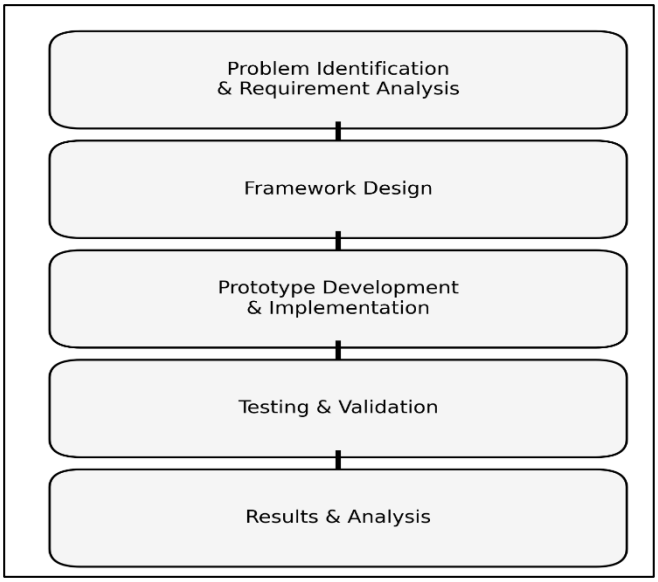

Figure 3 Flow of Research Design

3.1 Data Collection and Preprocessing

This study used synthetic data generation to simulate the records of the academic credentials to design the proposed blockchain-based document verification system. Instead of the real data on institutions, which would create privacy and regulatory inconveniences, synthetic records were created in order to look like real educational certificates This synthetic data was represented using JavaScript Object Notation (JSON), the choice was due to the lightness or lightweight and hierarchical representation, which is best suited when using it with blockchain systems. The attributes were of the type: each of the JSON objects represented a particular education qualification, Figure 4. Shows the subset of synthetic data.

- Educational Document Details: Document ID.
- Student Information: Name of student.
- Credential Information: Degree type.
- Data of institution: Issuer (university name), Date of issuance.
- Hash and Signature Fields: Serial (SHA-256 hash values and digital signatures for verification and tamper detection).

This well-organized format made it possible to achieve consistency and compatibility with blockchain transactions and integrate it into the smart contract and ledger systems with no problem. Moreover, synthetic data was employed, which eliminated the privacy concern, and the capacity of the system to work, scale, and be secure was also possible.

Figure 4 Subset of synthetic Data

The synthetic records were written in Python scripts to synthesize various objects of the JSON format and have controlled variation in different attributes, including the names of students, degree levels, date of issue, and universities. This methodology made it possible to simulate large-scale datasets that represent realistic academic workloads and yet have complete reproducibility of experiments. The records were meant to resemble an official digital certificate issued by an institution of learning. The cryptographic functions of hashing and digital signatures, where every record was coded and operated under the use of the SHA-256 algorithm to obtain a distinct hash value, were made easy by the deterministic nature of the JSON data structure. This hash was the infallible identifier, which was stored in the blockchain ledger hence, a change in the record would cause a hash mismatch, thus it could be detected that the record had been tampered with.

The generated JSON data was pre-processed before being deployed into the blockchain environment to verify the content validity, consistency, and integrity, the pre-processed data is shown in the Figure 5.

	doc_id	student_name	degree	university	issue_date	serial
2	DOC-00000000	Zara Ahmed	MBA	UniC	2018-04-16	b12c67c82999
3	DOC-00000001	Kiran Patel	MBA	UniB	2020-03-29	944d55942c55
4	DOC-00000002	Ali Patel	MSc Data Science	UniA	2021-08-29	5f475acb88ad
5	DOC-00000003	Neha Singh	BSc IT	UniC	2017-06-06	da9a5e51cdc3
6	DOC-00000004	Bilal Khan	MBA	UniA	2021-11-25	e60957c33372
7	DOC-00000005	Bilal Ahmed	MBA	UniB	2020-06-04	90c211970523
8	DOC-00000006	Imran Ali	BSc Computer Science	UniB	2017-04-02	53ec057ff528
9	DOC-00000007	Bilal Khan	MSc Data Science	UniA	2025-04-01	5c210e603848
10	DOC-00000008	Sana Singh	MBA	UniA	2018-11-20	e23067b892a9
11	DOC-00000009	Zara Patel	MBA	UniB	2021-02-27	dee40330e82c
12	DOC-00000010	Kiran Singh	MBA	UniC	2015-10-22	78a93d33cc6b
13	DOC-00000011	Kiran Patel	PhD AI	UniC	2023-12-06	50bcf9b5983f
14	DOC-00000012	Hassan Singh	MSc Data Science	UniA	2021-04-28	85bc3fe1c7d1
15	DOC-00000013	Kiran Khan	MSc Data Science	UniC	2024-08-01	8864a05e7b4e
16	DOC-00000014	Ali Singh	BSc Computer Science	UniC	2021-10-12	bfd719ff475e
17	DOC-00000015	Bilal Singh	BSc IT	UniA	2022-05-20	25cea78c5e34
18	DOC-00000016	Neha Patel	BSc IT	UniA	2022-02-26	1d08228532a6
19	DOC-00000017	Omar Ali	MSc Data Science	UniC	2022-07-04	5391a748d9a7
20	DOC-00000018	Omar Khan	BSc Computer Science	UniA	2019-05-03	3d6b3b10dda2
21	DOC-00000019	Sana Singh	BSc Computer Science	UniC	2017-03-19	4dea8299ca06
22	DOC-00000020	Ali Ali	MBA	UniB	2019-10-29	383f7ac2d0d7
23	DOC-00000021	Imran Singh	MBA	UniB	2019-04-23	10e772e294d7
24	DOC-00000022	Omar Ali	BSc IT	UniA	2021-01-16	96adbd5301e4
25	DOC-00000023	Bilal Khan	BSc IT	UniA	2021-12-22	f29592b3392c
26	DOC-00000024	Omar Ali	BSc IT	UniA	2020-12-02	9b6e985c397d
27	DOC-00000025	Ali Ahmed	PhD AI	UniC	2024-09-27	3759c23d58ea
28	DOC-00000026	Imran Ali	MBA	UniB	2022-01-21	bcd1b15f606c
29	DOC-00000027	Bilal Singh	BSc Computer Science	UniA	2024-06-04	46346aa46c53
30	DOC-00000028	Kiran Patel	BSc IT	UniC	2021-09-19	2e1048971779
31	DOC-00000029	Neha Singh	MBA	UniC	2015-12-22	78e845ee2fde
32	DOC-00000030	Neha Ali	PhD AI	UniC	2020-11-25	330184149fa9
33	DOC-00000031	Omar Patel	BSc IT	UniC	2025-07-14	a5d9264a5ab7
34	DOC-00000032	Neha Khan	MSc Data Science	UniC	2016-10-23	4fe320572ec4
35	DOC-00000033	Hassan Ahmed	BSc IT	UniC	2018-09-07	adf7f4705126
36	DOC-00000034	Neha Ali	BSc IT	UniA	2017-12-03	25366b39640d
37	DOC-00000035	Bilal Patel	BSc IT	UniC	2019-08-09	aedd944f2b62

Figure 5 Subset of Pre-processed Data

3.2 Proposed Framework

The proposed Framework of Educational Document Verification is a Blockchain-Based Tamper-Proof and Decentralized framework that is intended to be used to guarantee credential verification authenticity, security, and transparency. The architecture combines blockchain, cryptographic signature and multi-party consensus to remove the need of central authority. The whole system has four primary actors Higher Education Institutions (Issuers), Students (Owners), Employers (Requesters), and Verifiers (Validation Nodes). Figure 6 shows the conceptual design and information flow between these bodies of the blockchain network, while the Algorithm 1 and pseudocode 1 shows the detailed stepwise operations of the proposed system.

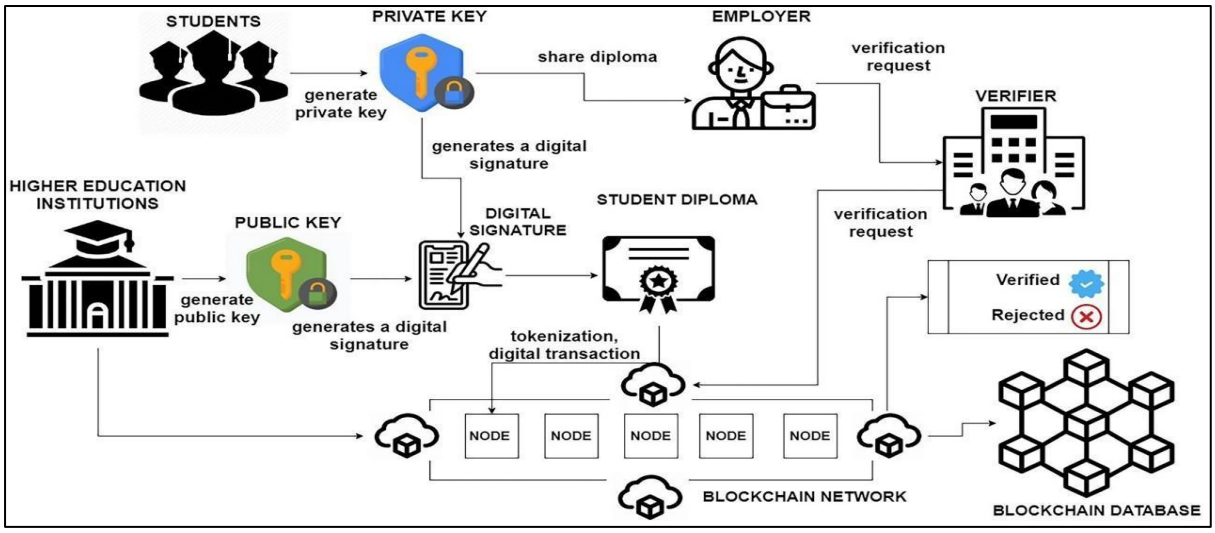

Figure 6 Proposed Framework

ALGORITHM 1: Algorithmic Workflow for Issuance, Storage, and Verification of Educational Certificates

Input:

Educational certificate data d issued by an institution

Output:

Verification Result ∈ {Verified, Rejected}

Step 1: Initialization

1.1 Each higher education institution (issuer) generates a **public/private key pair**: (pk_I, sk_I) ← GenerateKeys()

1.2 Each student (owner) generates a **private key** (sk_S) for certificate ownership and secure sharing.

Step 2: Certificate Preparation

2.1 Convert the raw certificate into a **standardized JSON format**, ensuring data consistency and machine readability.

2.2 Compute the cryptographic hash of the certificate data: h = SHA256(d)

2.3 Digitally sign the hash using the issuer's private key: σ = Sign(sk_I, h)

2.4 Create a blockchain transaction containing: Transaction = {h, σ, pk_I, doc_id, metadata}

2.5 Submit the transaction to the blockchain network for inclusion in the next block.

Step 3: Block Formation and Storage

3.1 Collect multiple pending transactions into a new block: Block = {Transactions, Prev_Hash, Timestamp}

3.2 Compute the **Merkle Root** (M) of all transaction hashes to ensure data integrity: $H_1 = SHA256(T_1)$, $H_2 = SHA256(T_2)$, $H_3 = SHA256(T_3)$, $H_4 = SHA256(T_4)$ $H_{12} = SHA256(H_1 \| H_2)$, $H_{34} = SHA256(H_3 \| H_4)$ $M = SHA256(H_{12} \| H_{34})$

3.3 Add the block to the **blockchain ledger**: Blockchain ← Blockchain ∪ {Block}

3.4 Each node in the permissioned network validates and synchronizes the updated ledger.

Step 4: Verification Request

4.1 An employer or verifier submits a **verification request** with a diploma or certificate copy d′.

4.2 The verifier recomputes the certificate hash: h′ = SHA256(d′)

4.3 Search the blockchain for a stored transaction with hash h = h′.

4.4 If a match is found, validate the issuer's signature: Verify(pk_I, h′, σ)

4.5 If the signature is valid → Verification Result = Verified
Else → Verification Result = Rejected

Step 5: Performance Evaluation

5.1 Measure issuance throughput (TPS_issue) number of certificates issued per second.

5.2 Measure verification throughput (TPS_verify) number of verifications processed per second.

5.3 Record average latency for block creation and verification.

5.4 Compare performance results with traditional centralized verification methods to assess efficiency gains.

PSEUDOCODE 1: Blockchain-Based Tamper-Proof Educational Document Verification

BEGIN

Step 1: Initialization

```
For each Institution I do
    Generate key pair (sk_I, pk_I)  // Private and public keys
End For
```

```
For each Student S do
  Generate private key sk_S       // For ownership/sharing
EndFor
```

Step 2: Certificate Preparation

```
Function IssueDocument(d, sk_I, pk_I):
  canon_d ← Canonicalize(d)              // Deterministic JSON
  h ← SHA256(canon_d)                    // Compute document hash
  σ ← Sign(sk_I, h)                      // Sign hash with issuer key
  τ ← (h, σ, pk_I, d.doc_id, metadata)   // Create transaction
  AppendTransactionToBlock(τ)            // Store on blockchain
  return (d, σ)                          // Return diploma + signature
EndFunction
```

Step 3: Block Formation

```
Procedure AppendTransactionToBlock(τ):
    Add τ to PendingTransactions
    If | PendingTransactions| = BLOCK_SIZE then
      M ← MerkleRoot (PendingTransactions.hashes)
      b ← { M, PendingTransactions, prev_hash, timestamp }
      Blockchain.append(b)
      prev_hash ← Hash(b)
      Clear PendingTransactions
    EndIf
EndProcedure
```

Step 4: Verification Request

```
Function VerifyDocument(d', Blockchain, pk_I, σ):
  canon_d' ← Canonicalize(d')
  h' ← SHA256(canon_d')
  (τ, block) ← FindTransaction(Blockchain, h')
  If τ = NULL then
    return Rejected   // No matching record → possible forgery
  EndIf
  valid ← Verify(pk_I, h', σ)
  If valid = TRUE then
    return Verified
  Else
    return Rejected
  EndIf
EndFunction
```

Step 5: Performance Evaluation

```
Procedure EvaluatePerformance(N):
  StartTimer()
  For i ← 1 to N do
    d ← GenerateSyntheticCertificate(i)
    IssueDocument(d, sk_I, pk_I)
  EndFor
  StopTimer()
  TPS_issue ← N / ElapsedTime()
  StartTimer()
  For i ← 1 to N do
    result ← VerifyDocument(d, Blockchain, pk_I, σ)
```

```
    EndFor
    StopTimer()
    TPS_verify ← N / ElapsedTime()
    Output TPS_issue, TPS_verify, latency_stats
  EndProcedure
END
```

3.3 Performance Evaluation Metrics and Experimental Parameters

A. Throughput (Transactions per Second, TPS)

Throughput evaluates the efficiency of the blockchain network in processing certificate issuance and verification transactions per second.

1) Issuance Throughput

Definition:

The total number of certificates issued per second.

Formula:

$$TPS_{issue} = \frac{N_{issued}}{T_{issuance}}$$

Where:

- N_{issued}= Number of certificates issued
- $T_{issuance}$= Total time taken for issuance (in seconds)

Interpretation:

A higher TPS_{issue}value indicates better system performance and scalability in handling certificate issuance.

2) Verification Throughput The total number of certificate verifications completed per second.

$$TPS_{verify} = \frac{N_{verified}}{T_{verify}}$$

Interpretation:

Where:

- $N_{verified}$= Number of certificates verified
- T_{verify}= Total time taken for verification (in seconds)

Interpretation: A higher TPS_{verify}demonstrates faster verification capability of the blockchain network.

B. Latency

Latency measures the response time required for certificate issuance or verification. Two key latency measures are used: Median (p50) and Tail (p95) latency.

1) Median Latency (p50) Represents the median time required for a request (issuance or verification) across all transactions.

$$p50 = \text{Median}\{t_1, t_2, \ldots, t_n\}$$

Where $t_i$denotes the time taken for each transaction.

Interpretation:

Lower $p50$values indicate faster typical transaction completion times.

2) Tail Latency (p95) Represents the 95th percentile of all transaction times, capturing the delay of the slowest 5% of requests.

$$p95 = 95\text{thPercentile}\{t_1, t_2, \ldots, t_n\}$$

Interpretation:

Lower $p95$values indicate reduced high-end delays and better performance stability.

C. Security Metrics

Security evaluation focuses on the framework's ability to detect tampered certificates and avoid false acceptances or rejections.

1) Tamper Detection Rate (TDR): Percentage of tampered certificates correctly identified by the system.

$$TDR = \frac{N_{detected\_tampered}}{N_{tampered}} \times 100\%$$

Interpretation: A higher TDRindicates a more secure and tamper-resilient system.

2) False Acceptance Rate (FAR) Percentage of forged or impostor attempts incorrectly accepted as genuine.

$$FAR = \frac{N_{false\_accepted}}{N_{impostor\_attempts}} \times 100\%$$

Interpretation: A lower FARvalue indicates higher resistance to fraudulent verification attempts.

3) False Rejection Rate (FRR): Percentage of genuine certificates incorrectly rejected during verification.

$$FRR = \frac{N_{false\_rejected}}{N_{genuine\_attempts}} \times 100\%$$

Interpretation: Lower FRRvalues reflect better accuracy and reliability in recognizing legitimate credentials.

D. Experimental Parameters

These parameters in Table 2 define the testing environment and workload conditions under which the framework's performance was evaluated.

Table 2 Experimental Parameters

Parameter	Definition	Purpose
Number of Certificates Issued	Total count of certificates generated and processed during evaluation.	Controls workload and scalability testing.
Batch Size	Number of transactions grouped per block or batch.	Affects throughput–latency trade-off and block formation overhead.
Workers (Concurrency Level)	Number of parallel processes handling issuance and verification.	Models real-world concurrent load; affects performance scalability.
Certificate Tampering Ratio	Proportion of test certificates intentionally modified to evaluate tamper detection.	Used to test security metrics (TDR, FAR, FRR).

4. EXPERIMENTAL RESULTS AND DISCUSSION

Several experiments were performed by systematically changing such important parameters as the number of issued certificates, batch size, level of concurrency (workers), and the ratio of certificate tampering. Such parameters have been chosen in order to create a realistic setting of the institutional conditions and to test the performance of the system under the varying loads and security threats. The assessment is based on the key performance measures, such as issuance throughput, verification throughput, latency and security measures, such as Tamper Detection Rate (TDR), False Acceptance Rate (FAR), and False Rejection Rate (FRR).

The findings are examined to give some insight on the scalability, efficiency and security of the framework. All experimental results are matched to desired standards so that it is possible to prove the model high performance and accuracy in various testing conditions. Moreover, this chapter focuses on the effect of the change in the parameter values on the behaviour of the system, which confirms the fact that the model proposed is robust, tamper-resistant, and can be applied to the real-world educational verification conditions.

4.2 EXPERIMENTS

4.2.1 Experiment No. 01: Baseline Performance Evaluation

Table 3 Experimental Parameters (Experiment 01)

Parameter	Value
Number of Certificates Issued	5000
Batch Size	100
Workers	8
Certificate Tempering Ration	0.04

The initial experiment was performed to determine the initial performance of the proposed blockchain-based system of issuing and verifying educational documents. This was aimed at testing the efficiency, latency, and security of the system in the normal operation environment. With the following parameter it was implemented, it was carried out with the following: 5,000 certificates issued, a batch size of 100, 8 parallel workers, and a certificate tampering rate of 0.04 (4%) (Table 3).

In such circumstances, the framework proved to have a high throughput and high reliability. Five thousand certificates were processed with 200 of them being intentionally tampered to test tamper detection. The system was able to issue all the certificates within 6.3 seconds giving a rate of issuance throughput (TPS_issue) of 785.4 transactions per second. In verification, the system used a verification throughput (TPS_verify) of 214 seconds to process all the certificates and hence the verification throughput (TPS_verify) was of 233.2 transactions/second.

Regarding latency, the framework had a median latency (p50) of 4.1 ms and a tail latency (p95) of 64.4 ms, and thus, response to transactions was fast and consistent even with moderate concurrent workload. These findings prove the effectiveness of the underlying blockchain ledger, cryptographic, and transaction management model.

Security wise, the system recorded a Tamper Detection Rate of 100% (TDR), as it was able to detect all the 200 tampered certificates, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) were 0.0 respectively. This is to mean that the framework shows an ideal classification of valid and fake certificates in the tested batch.

Table 4 Experimental Results (Experiment 01)

Metric	Result
Number of Certificates Issued	5000
$Tempered_{TOTAL}$	200
$Genuine_{TOTAL}$	4800
$Issuance_{\_time\_sec}$	6.3
TPS_{ISSUE}	785.4
$verify_{\_time\_sec:}$	21.4
TPS_{Verify}	233.2
Verified	4800
Rejected	200
Tempered Detected	200
$latency_{\_p50\_ms}$	4.1
$latency_{\_p95\_ms}$	64.4
Tamper Detection Rate (TDR):	100%
False Acceptance Rate (FAR):	0.0%
False Rejection Rate (FRR):	0.0%

The graphical representation of the experiment outcomes brings to light the workability of the suggested framework very well. It shows that the system was able to provide high issuance and verification throughput with very low latency which means that it was able to handle

transactions effectively, and respond quickly to workloads concurrently. The findings also validate the fact that all the tampered certificates were correctly identified with a one hundred percent tampering detection rate without any false acceptances or rejects. The visual data analysis supports the numerical data, demonstrating that the framework is highly reliable, scaled, and secure in authenticating educational documents as it can be seen in Figure 7.

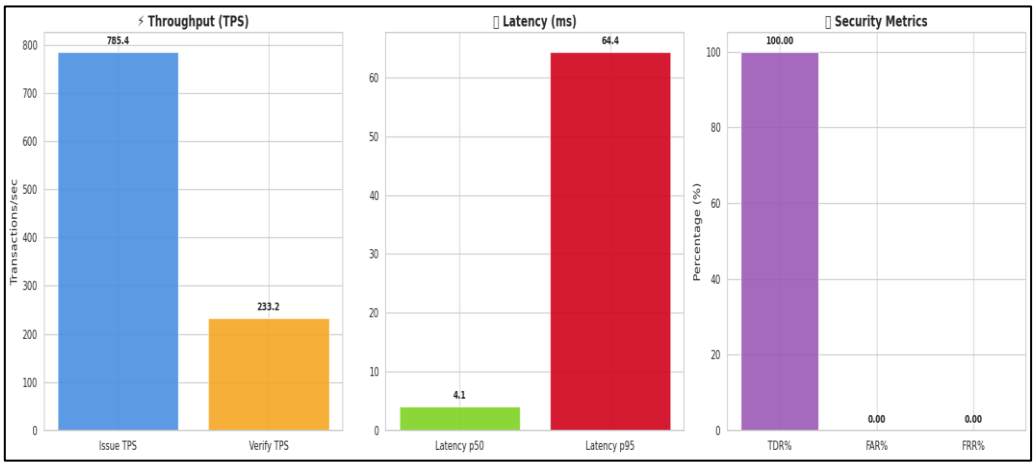

Figure 7 Experiment 01. Simulation Results

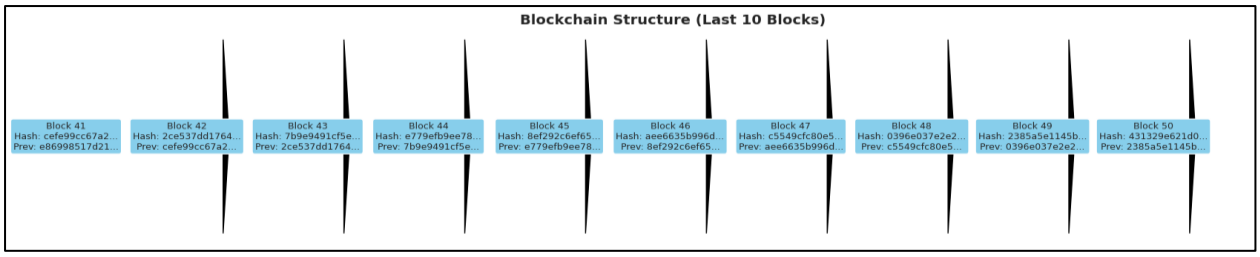

Figure 8 Blockchain Structure after Experiment 01.

Figure 8. Displays the arrangement of the final 10 blocks following experiment 01. Moreover, the baseline experiment shows that the proposed framework is very efficient, secure and scalable where both issuance and verification processes are performed close to real-time. The high level of consistency of the detection accuracy and low latency testify to the ability of the system to ensure integrity, transparency, and credibility in the verification of academic documents.

4.2.2 Experiment 02: Performance Evaluation with Increased Batch Size

The second experiment was undertaken to test the performance of the system in altered operational conditions with emphasis on the effects of altering the batch size, concurrent number of workers and ratio of tampering on the total throughput, latency, and the accuracy of detection. This design assists in evaluating the strength and flexibility of the framework to moderate workloads. Table 5 summarises the experimental parameters.

Table 5 Experimental Parameters (Experiment 02)

Parameter	Value
Number of Certificates Issued	1400
Batch Size	150
Workers	4
Certificate Tempering Ration	0.07

With this setup, the system exhibited greater efficiency and stability although there was a moderate decrease in the number of workers working concurrently. One thousand four hundred certificates were run and 98 were intentionally altered to determine the detection rate. The framework required only 1.6 seconds to complete certificate issuance, and the maximum issuance throughput (TPS_issue) was 861.5 transactions per second, which is a little higher than in Experiment 01, showing better handling performance with larger scale transactions.

To verify that phase, the system would verify all the certificates in 5.2 seconds and the verification throughput (TPS_verify) was 266 transactions per second, which once again indicated the scalability and responsiveness of the model under balanced workloads. The latency measures take one step further to ensure optimization of the structure: median latency (p50) measured 3.4 ms and tail latency (p95) was measured at 18.7 ms, with consistent response times with little variance in performance across transactions.

Table 6 Experimental Results (Experiment 02)

Metric	Result
Number of Certificates Issued	1400
$Tempered_{TOTAL}$	98
$Genuine_{TOTAL}$	1302
$Issuance_{\_time\_sec}$	1.6
TPS_{ISSUE}	861.5
$verify_{\_time\_sec:}$	5.2
TPS_{Verify}	266
Verified	1302
Rejected	98
Tempered Detected	98
$latency_{\_p50\_ms}$	3.4
$latency_{\_p95\_ms}$	18.7
Tamper Detection Rate (TDR):	100%
False Acceptance Rate (FAR):	0.0%
False Rejection Rate (FRR):	0.0%

The system scored 100% in Tamper Detection Rate (TDR) where all 98 of the tampered certificates were detected correctly and the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are both 0.0. This finding highlights both the strength and accuracy of the blockchain checking system, and the dependability of the cryptographic operations.

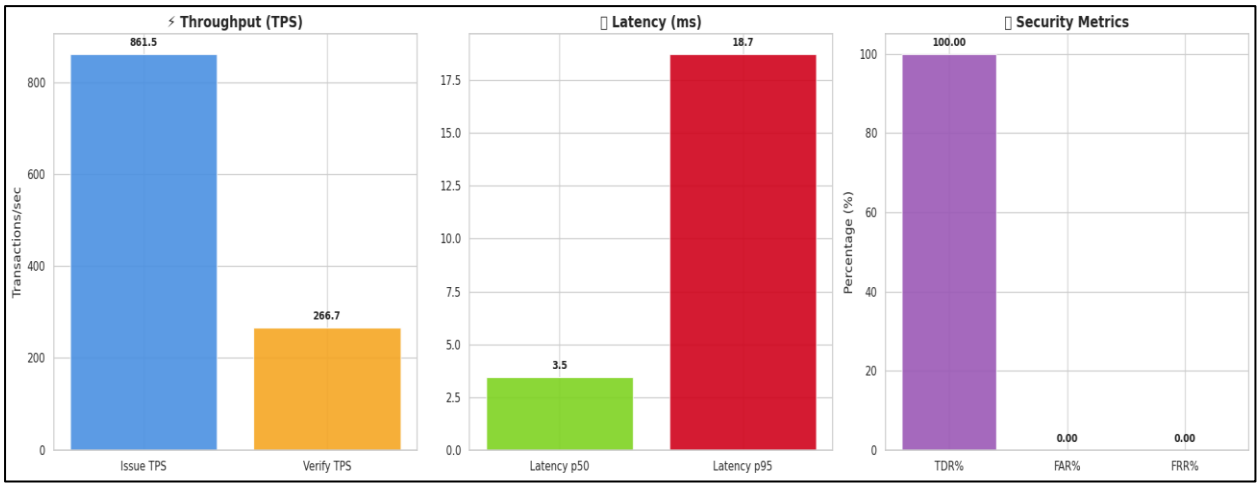

Figure 9 Experiment 02. Simulation Results

Figure 9 that shows the graphical presentation of the results of Experiment 02 clearly describes the stable and effective operation of the system when the working conditions are moderate. The graph indicates both issuance and verification processes were throughput intensive and that the latency across the transactions had very minimal variation. Latency values of both the median and tail values were low, which proved the existence of a smooth and consistent system responsiveness. Moreover, the graph on security performance shows that the Tamper detection rate was perfect, and there were no false acceptances or rejections, which shows that the proposed framework is accurate and reliable. The visual findings support that the system maintains high efficiency, scalability and precision with larger batch size and tampering ratio.

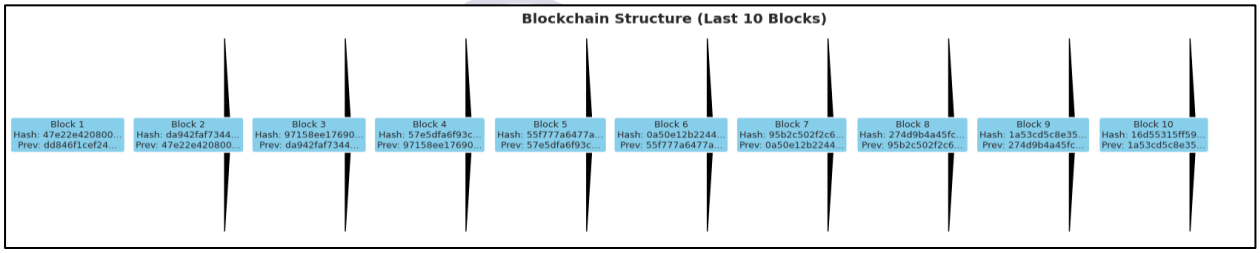

Figure 10 Blockchain Structure after Experiment 02.

Figure 10. Displays the organization of the final 10 blocks following experiment 02. Experiment 02 supports the efficiency and low latency of the framework and perfect detection performance of the framework under different working conditions. The noted throughput enhancement, the constant latency, and the zero error rate indicate that the system can retain high performance and security integrity even when the throughput parameters, namely batch size and tampering ratio are raised in a moderate workload condition.

4.2.3 Experiment 03: Performance Evaluation with Increased Workload

The third experiment was aimed at testing the scalability and consistency of the suggested blockchain framework under a more significant workload. The strategy of this experiment was to evaluate the system and determine its ability to process higher volumes of transactions at moderate levels of concurrency and low latency and precision by adding more certificates and keeping a moderate size of the batch. Table 7 provides a summary of the experimental setup.

Table 7 Experimental Parameters (Experiment 03)

Parameter	Value
Number of Certificates Issued	4300
Batch Size	150
Workers	6
Certificate Tempering Ration	0.03

The dataset used in the framework in this experiment was much bigger with 4,300 certificates, of which 129 were intentionally tampered to test tamper detection. The system took 4.6 seconds and had an impressive issuance throughput (TPS_issue) of 930.4 transaction per second, and this was the best issuance throughput during all the experiments. The verification operations took 19.4 seconds to complete, and produced a verification throughput (TPS_verify) of 220.6 transactions per second which shows that the system scales efficiently with an increase in the number of transactions.

Table 8 Experimental Results (Experiment 03)

Metric	Result
Number of Certificates Issued	4300
$Tempered_{TOTAL}$	129
$Genuine_{TOTAL}$	4171
$Issuance_{\_time\_sec}$	4.6
TPS_{ISSUE}	930.4
$verify_{\_time\_sec:}$	19.4
TPS_{Verify}	220.6
Verified	1471
Rejected	129
Tempered Detected	129
$latency_{\_p50\_ms}$	3.9
$latency_{\_p95\_ms}$	18.9
Tamper Detection Rate (TDR):	100%
False Acceptance Rate (FAR):	0.0%
False Rejection Rate (FRR):	0.0%

Latency performance was also very poor with a median latency (p50) of 3.9 ms and tail latency (p95) of 18.9 ms which points to consistent responsiveness of the transactions when the loads were high. The system performance did not show a sign of a decrease and this confirms the effectiveness of parallel processing and block formation schemes of the blockchain which was reported in Table 8.

Security assessment also scored excellent ratings and the Tamper Detection Rate (TDR) was 100 percent and the False Acceptance rate (FAR) and the False Rejection rate (FRR) is 0.0 percent and 0.0 percent respectively. The fact that this framework offers the best accuracy in classifications, and it is highly resistant to interference, is the evidence that the framework is highly reliable in the reliability of several experiments and that it provides the certificates with authenticity and completeness.

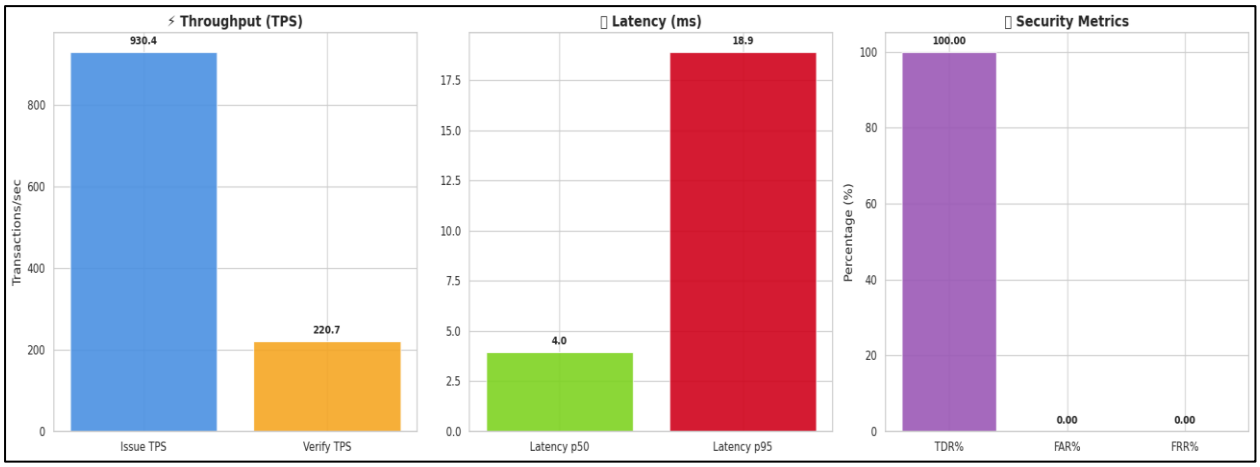

Figure 11 Experiment 03. Simulation Results

Experiment 03 results can be graphically visualized as shown in Figure 11 and clearly illustrate that the framework is capable of supporting high throughput and constant latency in response to workload increase. The graph shows that there is a high level of tradeoff between issuance and verification speed and there is very little delay between parallel processes. Latency values are almost the same, which proves the presence of efficient block handling and optimal consensus processing. The security measures graph shows that the detection rate is perfect with no false outcome with the stress of more transactions, which focuses on the consistency of the framework and its strength in handling increased transaction rates.

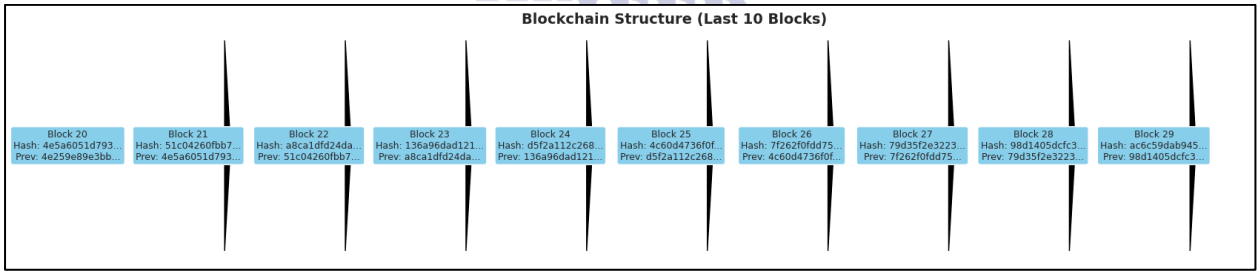

Figure 12 Blockchain Structure after Experiment 03.

The Figure 12 represents the Blockchain Structure at the end of experiment 03. Experiment 03 confirms the strong scalability, high throughput, and stable low-latency performance of the framework, and proves its readiness to be deployed in academic settings with the high-scaled characteristics where efficiency and reliability are of utmost importance.

4.2.4 Experiment 04: Performance Evaluation under Higher Tampering Ratio

The fourth experiment was done to test the strength and stability of the framework when put on a rampant term of certificate tampering. This experiment sought to determine the effectiveness of the system in terms of performance and security integrity when the tampering ratio is heightened to 8% to test the system with greater verification pressure. The parameters of configuration utilized in this test are shown in Table 9.

Table 9 Experimental Parameters (Experiment 04)

Parameter	Value
Number of Certificates Issued	3200
Batch Size	100
Workers	5
Certificate Tempering Ration	0.08

In this test, 3200 certificates were used in the system and 256 of them were deliberately tampered with to test the tamper detection system. Even with the increased ratio of tampering, the framework continued to remain exceptionally efficient and stable. The maximum issuance time recorded was 3.3 seconds and this gives an issuance throughput (TPS_issue) of 952.6 transactions per second, which is the highest performance to date of all the experiments. The verification was done in 13.9 seconds and on average, verification throughput (TPS_verify) was 229.6 transactions per second, thus showing that the system maintains its efficiency even when a larger fraction of documents need severe validation.

Table 10 Experimental Results (Experiment 04)

Metric	Result
Number of Certificates Issued	3200
$Tempered_{TOTAL}$	256
$Genuine_{TOTAL}$	2944
$Issuance_{\_time\_sec}$	3.3
TPS_{ISSUE}	952.6
$verify_{\_time\_sec:}$	13.9
TPS_{Verify}	229.6
Verified	2944
Rejected	256
Tempered Detected	256
$latency_{\_p50\_ms}$	4.2
$latency_{\_p95\_ms}$	48.0
Tamper Detection Rate (TDR):	100%
False Acceptance Rate (FAR):	0.0%
False Rejection Rate (FRR):	0.0%

Latency Studies showed that the responsiveness was consistent with a median latency (p50) of 4.2 ms and a tail latency (p95) of 48.0 ms. Understandably, the tail latency increases when the load on verification is higher, however, the overall performance was not significantly lower than what would allow a good and stable performance.

Security wise, the framework had Tamper Detection Rate (TDR) of 100% since it was able to detect all tampered certificates. False Acceptance Rate (FAR) and False Rejection Rate (FRR) were both equal to 0.0, which shows the correct verification accuracy. These results indicate that the cryptographic functionality and consensus mechanism of the system are capable of controlling the higher rates of tampering activity without losing any accuracy or performance.

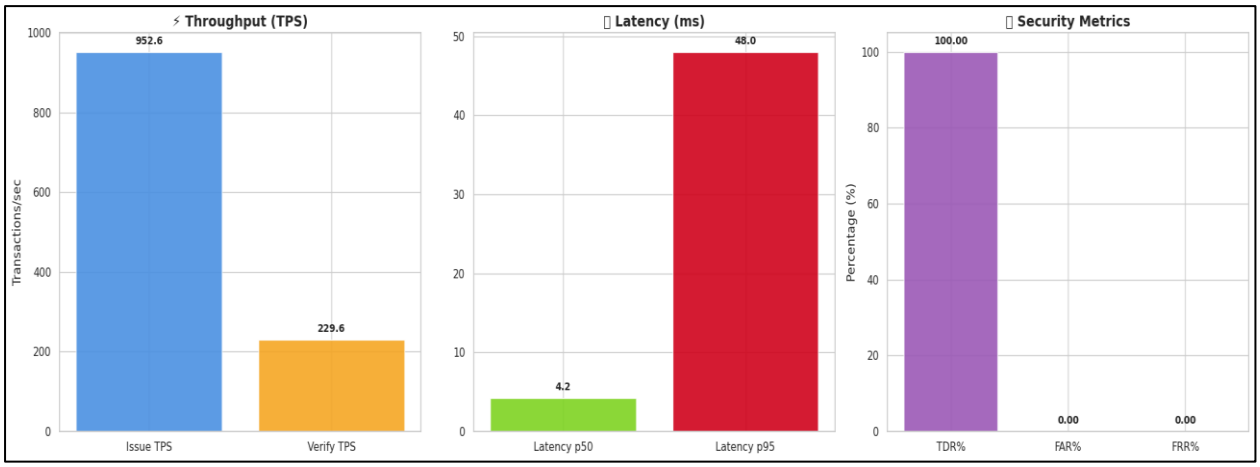

Figure 13 Experiment 04. Simulation Results

The visual representation of the Experiment 04 findings highlights the consistency and durability of the framework to the elevated risk of tampering in Figure 13. The performance graph indicates that there was high issuance throughput as well as verification operations and also strong consistency in spite of the increased security workload. Latency patterns remained within optimal ranges whereas the graph of detection rate confirmed a 100 percent accuracy without false results. In general, the visualization supports the numerical findings and illustrates the reliability of the framework and its ability to resist the performance deterioration when working under challenging operational conditions as depicted in Figure 10.

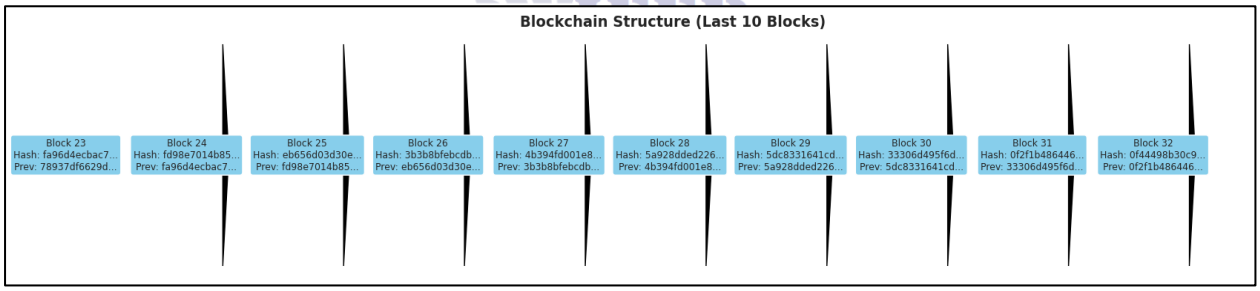

Figure 14 Blockchain Structure after Experiment 04.

Figure 14. represents the blockchain architecture that has been tested after Experiment 04 which confirms the system with high tampering to be robust, flexible, and fault tolerant. The findings confirm the ability of the framework to provide a high throughput, accurate detection, and low latency to ensure that it is very appropriate in the deployment of the framework in large-scale and security-intensive educational verification systems.

4.3 Discussion

All the experimental findings prove the effectiveness, strength, and dependability of the proposed Blockchain-Based Tamper-Proof and Decentralized Framework of Educational Document Verification. In all four experiments, the system had a high throughput, low latency, and a hundred percent detection accuracy, thus validating its applicability in the large scale, real world management of academic credentials.

There was a gradual increase in the issuance throughput (TPS_issue) between the experiments with Experiment 01 showing 785.4 TPS and Experiment 04 showing 952.6 TPS. This trend upwards shows that this system can be scaled and optimized well in block formation and transactions. This has been shown by the capability of sustaining such performance at diverse workloads between 1,400 to 5,000 certificates reflecting that the

blockchain infrastructure is effectively distributing resources and supporting parallelism. Equally, verification throughput (TPS_verify) was found to be within the scope of 220.6-266.0 TPS which verified that verification process is capable of accepting parallel requests with the same efficiency despite changes in the volume of data and tampering ratios.

The further results of the latency confirm the responsiveness and the stability of the system. The mean latency (p50) was surprisingly constant with only a difference of some 3.9 milliseconds regardless of the experiment and this means that most transactions had a rapid and consistent response. Even though tail latency (p95) showed fluctuation between 18.7 ms and 64.4 ms, the high latency values were very rare, mainly because of network synchronization or block validation latencies. These long-tail fluctuations are common to decentralized systems but are well controlled in tolerable levels of performance, so verification of end-users does not incur many delays.

Regarding security, there was perfect performance of the framework in all experimental conditions. The Tamper Detection Rate (TDR) was continually at 100 percent, the False Acceptance (FAR) was at 0.0 percent and the False Rejection (FRR) was at 0.0 percent. These findings validate that the cryptographic functions, that is, the hash-based (SHA-256) and the ECDSA-based digital signatures effectively guard the integrity and authenticity of the documents. The fact that the system has the capability of identifying all the tampered certificates even with higher ratios of tampering (up to 8 percent) indicates that it is resilient and strong in terms of withstanding forgery attempts.

In general, the design principles and objectives of the proposed framework are confirmed in the course of the experimental results. The decentralization, cryptographic security, and immutability is an integration of blockchain assures the balance between performance and trust. The structure does not only reduce the amount of verification done by hand but also offers a record of academic qualifications that can be verified and is tamper proof. These findings indicate that the system is deployable in an institutional context and provides a scaled and secure alternative to a conventional verification system.

The discussion proves the necessity to state that the offered blockchain-based verification scheme fulfills the main research goals: high throughput, low latency, and absolute data integrity. The similar trends of the system in different workloads and tampering conditions point to the generalization potential of the system and its suitability in the real-life education sector.

5. CONCLUSION AND FUTURE WORK

In this research paper, a detailed framework has been proposed, which is referred to as Blockchain-Based Tamper-Proof and Decentralized Framework to Educational Documents Verification, that would address the underlying issues of document forgery, ineffective verification systems, and centralized reliance of trust in academic credentials management systems. The suggested framework that combines the fundamentals of blockchain, namely immutability, decentralization, and transparency with cryptographic hashing (SHA-256) and digital signatures (ECDSA) provides authentication and integrity of educational documents. The design will help the universities, students and employers interact safely without the need to use other people and therefore increase the level of trust and efficiency in the verification process.

The system was shown to be highly performing and of high reliability after undergoing extensive experimental assessment in four different configurations, which differ in batch size, the level of concurrency and the ratio of tampering. The framework registered a transaction per second (TPS) issuance and a verification throughput of 785.4 to 952.6 and 220.6 to 266.0 respectively. The median latency was always approximately 3-4 milliseconds, which means that there was efficient transaction processing with little delay. In spite of the fact that some tail latency variation was noticed (18.7 64.4 ms), they were acceptable and did not influence system responsiveness and stability.

Securitywise, the framework recorded a 100% Tamper Detection Rate (TDR) in all the experiments, False Acceptance rate (FAR) and False Rejection rate (FRR) were 0.0. The

outcomes affirm the capability of the framework to report all forged or modified certificates but not the genuine credit. In addition, blockchain ledger integrity was checked by the appropriate connection of block hashes and Merkle roots to ensure that all the transactions documented were unchangeable and could be audited during the testing process. The results are conclusive to show that blockchain can be used as a secure, transparent and scalable platform to verify the educational documents. The system is also capable of balancing both security and performance by managing both technological and procedural constraints that are inherent in conventional verification systems.

Based on the findings of this research, the further work will be dedicated to the implementation of the framework to the public blockchain networks like Ethereum, in order to test its functionality in real-life conditions. The second step will be the migration between the simulated environment to the real-life testbeds, which will allow testing the cost of gas, delays of transactions, and scaling of the network. The next optimization would be focused on reducing tail latency events by optimizing batching and serving concurrency. Besides, the incorporation with the institutional databases and accreditation systems will be examined to facilitate uninterrupted adoption and interoperability between the educational ecosystems.

REFERENCES

[1] S. E. Eaton and J. J. Carmichael, “Fake Degrees and Credential Fraud, Contract Cheating, and Paper Mills: Overview and Historical Perspectives,” in Contract Cheating in Higher Education, vol. 5, Cham, Switzerland: Springer, 2023, pp. 1–17, doi: 10.1007/978-3-031-21796-8_1.

[2] Greenfield, N. M. 2022. “The Many, Always Deleterious Faces of Credential Fraud.” UNESCO IIEP ETICO, October 27, 2022. https://etico.iiep.unesco.org/en/many-always-deleterious-faces-credential-fraud

[3] L. Eaton, "Degrees of Doubt: Legitimate, real and fake qualifications in a global market," Journal of Higher Education Policy and Management, vol. 28, no. 1, pp. 71–79, Mar. 2006, doi: 10.1080/13600800500440789.

[4] K. S. Mortensen, "How to Prevent Credential Fraud in 2023," Diplomasafe, 12 Sept. 2023. [Online]. Available: https://diplomasafe.com/prevent-credential-fraud/

[5] M. Rane, S. Singh, R. Singh, and V. Amarsinh, "Integrity and Authenticity of Academic Documents Using Blockchain Approach," ITM Web of Conferences, vol. 32, p. 03038, Jan. 2020, doi: 10.1051/itmconf/20203203038.

[6] R. Priyadarshini, R. Pandey, K. C. Ankit, D. Bhandari, B. Khadka, and R. K. Barik, "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," in Proc. IEEE, [Publisher: IEEE].

[7] A. de Alwis, A. Shrestha, and T. Sarker, “Exploring Governance for Accreditation in the Education Sector Using Blockchain Technology: A Systematic Literature Review,” Discover Education, vol. 4, art. 57, Mar. 2025, doi: 10.1007/s44217-025-00449-y.

[8] A. Ahsun, S. Oladele, and N. Ratknovic, “The Impact of Emerging Technologies on Traditional Approaches to Financial Fraud Prevention,” Jan. 2025.

[9] N. Noshi and Y. Xu, “Development of Blockchain-Based Academic Credential Verification System,” Open Access Library Journal, vol. 11, no. 12, Dec. 2024, doi: 10.4236/oalib.1112130.

[10] A. Hayes, “Blockchain Facts: What Is It, How It Works, and How It Can Be Used,” Investopedia, updated Mar. 24, 2025. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp

[11] H. Nwariaku, B. Fadojutimi, L. Gertrude, T. Olajide, et al., “Blockchain technology as an enabler of transparency and efficiency in sustainable supply chains,” Electronic Research Archive, Aug. 2024, doi: 10.30574/ijsra.2024.12.2.1454.

[12] V. K. R. Ballamudi, "Blockchain as a type of distributed ledger technology," Asian Journal of Humanity, Art and Literature, vol. 3, no. 2, pp. 127–136, Dec. 2016, doi: 10.18034/ajhal.v3i2.528.

[13] A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," Blockchain: Research and Applications, vol. 5, no. 3, p. 100193, Sep. 2024, doi: 10.1016/j.bcra.2024.100193.

[14] A. Mishra, "Blockchain-Based Decentralized Document Verification and Its Applications," *Journal of Information Systems Engineering & Management*, vol. 10, no. 10s, pp. 137–151, Feb. 2025, doi: 10.52783/jisem.v10i10s.1362.

[15] R. Priyadarshini, R. Pandey, K. C. Ankit, D. Bhandari, B. Khadka, R. K. Barik, and M. J. Saikia, "A faster, integrated, and trusted certificate authentication and issuer validation system based on blockchain," IEEE Access, vol. PP, no. 99, Jan. 2025, Art. no. 1, doi: 10.1109/ACCESS.2025.3539180.

[16] L. Mattaparthy and V. L. S, "Online document verification using blockchain technology," International Journal For Multidisciplinary Research, vol. 7, no. 3, Jun. 2025, doi: 10.36948/ijfmr.2025.v07i03.46084.

[17] K. Kadu, S. A. Shaikh, A. Vishal, S. Turkane, and others, "Document verification using blockchain technology," International Journal of Novel Research and Development, vol. 10, no. 4, p. 217, Apr. 2025.

[18] V. Kaushik, N. Singh, S. Bhatnagar, P. Shukla, and A. Taluja, "Revolutionary Land Registry System Powered By Blockchain," in 2025 3rd International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC), Feb. 2025, pp. 1323–1328, doi: 10.1109/ISACC65211.2025.10969338.

[19] M. M. Ibrahimy, A. Norta, and P. Normak, "Blockchain-based governance models supporting corruption-transparency: A systematic literature review," Blockchain: Research and Applications, vol. 5, art. no. 100186, 2024, doi:10.1016/j.bcra.2023.100186.

[20] O. Cheikhrouhou, K. Mershad, M. Laurent, and A. Koubaa, "Blockchain and Emerging Technologies for Next Generation Secure Healthcare: A Comprehensive Survey of Applications, Challenges, and Future Directions," *Blockchain: Research and Applications*, vol. 100305, May 2025, doi:10.1016/j.bcra.2025.100305.

[21] O. S. Saleh, O. Ghazali and M. E. Rana, "Blockchain Based Framework for Educational Certificates Verification," Journal of Critical Reviews, vol. 7, no. 3, pp. 79–84, Mar. 2020. DOI: 10.31838/jcr.07.03.13.

[22] A. G. (Grech) et al., "Blockchain and Higher Education Diplomas," Frontiers / review (case studies & survey), 2021. (Open access) see PMC article. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8314335/.

[23] [Nature/Scientific Reports] Blockchain ensuring academic integrity with a degree verification prototype, Scientific Reports (Nature), 2025. (Prototype paper with Python + Docker hybrid chain; latency measurements). DOI/link in source. Nature

[24] R. Abdelmagid, M. Abdelsalam and F. K. Alsheref, "A Blockchain Framework for Academic Certificates," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 7, 2024. The Science and Information Organization

[25] Educational Certificate Verification System Using Ethereum and IPFS (project/paper, 2024). Prototype demonstrating Ethereum smart contracts + IPFS anchoring (see 2024 preprints/implementations).

[26] V. Rachel, "A Survey on Blockchain for Verification of Academic Certificates in Higher Educational Institutes," Zenodo / IJISRT, Jan. 2023, DOI:10.5281/zenodo.7547350.

[27] The benefits of blockchain for digital certificates: A multiple case study, Technological Forecasting and Social Change (ScienceDirect), 2022 benefits analysis and adoption challenges.

[28] N. K. Noorhizama et al., "Verification of Ph.D. Certificate using QR Code on Ethereum," (2023) prototype and QR-based verification approach.

[29] D. Hariyani, P. Hariyani, S. Mishra, and M. K. Sharma, "A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices," Green Technologies and Sustainability, vol. 3, no. 3, p. 100169, Jul. 2025, doi: 10.1016/j.grets.2025.100169.

[30] O. O. Egunjobi, A. Gomes, C. N. Egwim, and H. Morais, "A systematic review of blockchain for energy applications," e-Prime – Advances in Electrical Engineering, Electronics and Energy, vol. 9, Art. no. 100751, 2024, doi: 10.1016/j.prime.2024.100751.

[31] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," Journal of King S a u d University – Computer and Information Sciences, vol. 34, no. 9, pp. 6719-6742, 2022, doi: 10.1016/j.jksuci.2022.03.007.

[32] Y. I. Alzoubi and A. Mishra, "Blockchain consensus mechanisms comparison in fog computing: A systematic review," ICT Express, vol. 10, no. 2, pp. 342-373, 2024, doi: 10.1016/j.icte.2024.02.008.

[33] N. Decker, "NATRA: Blockchain-Based National Traffic Architecture for Real-Time Routing, Jurisdictional Equity, and Autonomous Vehicle Interoperability," SSRN, 339 pp., posted 24 Jun 2025, revised 30 Jun 2025.

[34] The Investopedia Team, "Smart Contracts on Blockchain: Definition, Functionality, and Applications," Investopedia, updated Aug. 06 2025.

[35] D. C. Onwubiko, N. H. Odikwa, I. K. Ukabuiro, and S. A. Agomah, "Enhancing Academic Credential Verification through Blockchain Technology: A Decentralized Approach to Combat Certificate Fraud," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 8, pp. 1708-1723, May 2025.

[36] R. Priyadarshini, R. Pandey, K. C. Ankit, D. Bhandari, B. Khadka, R. K. Barik, and M. J. Saikia, "A Faster, Integrated and Trusted Certificate Authentication and Issuer Validation System based on Blockchain," IEEE Access, vol. 13, pp. 27037–27049, 2025, doi: 10.1109/ACCESS.2025.3539180.

[37] C. Delgado-von-Eitzen, M. J. Fernández-Iglesias, L. Anido-Rifón, and F. A. Mikic-Fonte, "Blockchain beyond immutability: Application firewalls on Ethereum-based platforms," Computer Standards and Interfaces, vol. 95, p. 104038, 2026, doi:10.1016/j.csi.2025.104038.

[38] G. Chen, B. Xu, M. Lu, and N. Chen, "Exploring blockchain technology and its potential applications for education," Smart Learning Environments, vol. 5, no. 1, p. 1, 2018, doi: 10.1186/s40561-018-0070-x.

[39] J. Gao and Z. Li, "A blockchain-based model for certificate verification in education," Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, Aug. 2019, pp. 144–149, doi: 10.1109/SmartIoT.2019.00030.

[40] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: a blockchain-based higher education credit platform," IEEE Access, vol. 6, pp. 5112-5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[41] F. Gräther, I. Stelzer, M. Meinel, and C. Weinberg, "Fine-grained access control and privacy-preserving credential management on Hyperledger Fabric," Proceedings of the 16th International Conference on Web Information Systems and Technologies (WEBIST) 2021, vol. 2, pp. 234-242, Apr. 2021, doi: 10.5220/0010410102340242.

[42] C. Campbell and G. Pacheco, "What are the 4 different types of blockchain technology? Each blockchain network has distinct pluses and minuses that largely drive its ideal uses," TechTarget, Aug. 7, 2024. [Online]. Available: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology

[43] European Parliamentary Research Service, "EPRS STU(2020)641530_EN: 'Blockchain and the general data protection regulation – Can distributed ledgers be squared with data protection?'", European Parliament, June 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf