ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

Al-Noor Journal for Information Technology and Cybersecurity

https://jncs.alnoor.edu.iq/

Blockchain-Based Document Verification System

[1]Omar Ali Athab, [1]Ali Hussein Salim, [1]Ali Falah Hassan

[1]Al-Khwarizmi College of Engineering, University of Baghdad, Baghdad, Iraq

Article information

Article history:
Received: October, 22, 2025
Revised: November, 19, 2025
Accepted: December, 21, 2025

Keywords:
Blockchain
Ethereum
IPFS
Smart Contract
Solidity
Web3.js
Polygon Network
MetaMask Wallet

Correspondence:

Omar Ali Athab
omarali@kecbu.uobaghdad.edu.iq

Abstract

The manual process of issuance and validation of academic documents in Iraq has long been frustrating and time-consuming, risking the students losing their hard-earned certificates. It is clear that this calls for a new and unconventional technique to upgrade this archaic system. This is where innovation in blockchain technology provides a powerful, extendable, and private solution for processes of certification. Blockchain is a decentralized database or distributed ledger recording transactions or digital events across participating parties who have executed the transactions. With this understanding, we have come up with a groundbreaking management system for export and verification of academic certificates. In this system, we automated laborious processes of certification, reducing all the manual work necessary in certification processes and thus incredibly reducing the overall cost. The idea is straightforward; a certificate is issued by the university, it is uploaded and hashed into the IPFS for storage. A unique QR code is generated for verification. When a verifier presents a file or a QR code, our system compares the hash with those previously stored in the blockchain for its existence. If it exists, the corresponding certificate is retrieved from the IPFS while an absent hash will result in denied request. By leveraging the power of blockchain technology, our system ensures that academic documents are securely and efficiently validated; a means of freeing up time and resources of institutions. Our proposed solution aims to improve the efficiency and security of academic document issuance and verification in Iraq.

DOI: https://doi.org/10.69513/jncs.v2.i2.a11

1 .Introduction

Education is the backbone of modern civilization, and the credentials received by students are important for their professional and personal growth. Traditionally, the issuance and verification of documents such as degrees, transcripts, and certificates have been a labor-intensive process involving a lot of hectic on the part of educational institutions and employers. However, with the advent of blockchain technology, a newer era in issuance and verification of academic credentials is found [1]. It is time-consuming and sometimes risky to issue and verify academic credentials manually. The process will involve printing out, signing, and mailing documents, which may take up to many weeks or months to be effectively issued. Besides, the documents can be questioned for their authenticity because they are easily tampered with or forged [2]. In contrast, blockchain technology provides a secure and efficient way to issue and validate academic documents. Using a blockchain system, the academic institutions can store student records and issues the academic document as a digital asset. These digital assets are tamper-proof and can be easily verified by employers or other institutions [3]. Moreover, the blockchain network gives a decentralized platform devoid of reliance on third-party verification services. This generally makes the process of document issuance and validation not only smooth but also efficient, cost-effective, and attains complete transparency [4].

To summarize, whereas traditional manual academic document issuances and validations have served us well, blockchain technology introduces an absolutely revolutionary approach, decentrally executed, more airtight, efficient, and cost-effective. Educational institutions and employers must latch onto this innovation if their processes are to be relevant and

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

effective in the digital future regarding the issuance and validation of academic documents; it is now evident that the future of this industry lies with blockchain technology [1].

2 .LITERATURE SURVEY AND RESEARCH GAP

Early explorations from 2017-2018 installed blockchain technology as a possible answer for preventing educational credential fraud via leveraging its core properties of decentralization, immutability, and transparency [5]. The essential value proposition become to create a dispensed, tamper-evidence public ledger that could stable digital belongings like certificate, transferring past blockchain's preliminary use in cryptocurrencies [6]. Initial proposals expected systems where students should become the custodians of their very own academic facts, eliminating the want for institutional intermediaries and bulky manual verification methods [6]. Early frameworks, such as 'CredenceLedger', conceptualized permissioned blockchains to keep compact information proofs of instructional credentials, making them easily verifiable by using stakeholders and third-birthday celebration agencies [7]. These foundational structures targeted on organizing the core architecture for issuing and verifying legitimate files [8], frequently highlighting the comparison with inefficient paper-based totally procedures and the blessings of a steady, unalterable digital record that might be maintained at a minimal value [9]. However, those early works also acknowledged demanding situations, such as the complexities of handling public/private keys for authentication and the need to make certain person privateness [6].

Building on foundational standards, the 2019-2021 length witnessed the emergence of greater specific and platform-precise architectural frameworks for report verification. A substantial fashion become the adoption of permissioned blockchains like Hyperledger Fabric, which become desired for its suitability in institutional settings requiring controlled get right of entry to and privateness [10,11]. For example, the HEDU-Ledger gadget changed into proposed as a Hyperledger Fabric application for degree attestation among universities and better training commissions, making use of a private permissioned community to ensure transparency and confidentiality among recognized stakeholders [12]. Another framework, VECefblock, also utilized Hyperledger Fabric to create a countrywide-level certificates authentication system, emphasizing its permissioned nature as perfect for control via a central ministry even as still providing decentralized verification [12,13]. This device designated a comprehensive architecture along with off-chain neighbor-hood databases and a particular statistics mapping structure to unify records from diverse establishments [13]. Concurrently, other researchers persevered to leverage public blockchains like Ethereum, using clever contracts to automate the verification of certificates information saved on-chain [14]. Some of these Ethereum-based structures commenced integrating the InterPlanetary File System (IPFS) for off-chain storage of the real record files, with only the report's hash being recorded on the blockchain to enhance performance [15]. This duration also produced more holistic structures like 'Cerberus', which aimed to closely replicate the prevailing credential atmosphere while introducing novel capabilities consisting of on-chain credential revocation thru smart contracts and user-pleasant QR-code-primarily based verification that did no longer require customers to control cryptographic keys directly [12,16].

Recent advancements from 2022 onwards have targeted on growing extra sophisticated, person-centric, and privacy-retaining file verification ecosystems through integrating complementary technology. A dominant trend is the considerable adoption of the InterPlanetary File System (IPFS) for decentralized, off-chain storage of huge file documents, with best their cryptographic hashes stored on-chain to lessen fees and enhance machine performance [17,18]. This method permits verifiers to preview the actual certificate whilst keeping the integrity and scalability of the blockchain lower back-quit [19]. The idea of Self-Sovereign Identity (SSI) has additionally won large prominence, with frameworks designed to provide people whole manage over their digital identification and credentials [20,21]. These SSI-based systems utilize Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to allow users to manage their information in a non-public virtual wallet and proportion it selectively with verifiers without involving the original company in the verification manner [22]. Some present-day structures, like DocStone, offer customizable multi-domain registration offerings that may be configured for special use instances and blockchains [23]. Furthermore, the today's studies explore advanced privacy-retaining strategies which include zero-expertise proofs (ZKPs), which permit for credential verification without exposing any underlying touchy data [24], the usage of Non-Fungible Tokens (NFTs) as credentials [21], and the development of twin-blockchain architectures to segregate public and personal records [24]. These superior systems demonstrate a mature expertise of the sphere's challenges, transferring beyond easy evidence-of-lifestyles to create complete, consumer-centric ecosystems that prioritize protection, privacy, and interoperability.[19]

Foundational architectures from 2017–2018 furnished proof-of-idea designs but disregarded key sensible elements which includes cost, person revel in, and mainly credential revocation—a demand for real-international use [9,6]. This creates a studies

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

hole in adapting those early fashions with efficient, modern revocation mechanisms, inclusive of on-chain clever-agreement tactics used in recent structures like EAS [12,16], which support decentralized, obvious revocation with rapid reaction instances [25]. Existing paintings also remains constrained to theoretical or small-scale reviews, leaving a lack of large-scale deployment insights [26]. This work proposes a blockchain-based architecture that combines on-chain certificate anchoring with off-chain document storage using IPFS. The design emphasizes efficient revocation handling, institutional governance, and deployment practicality.

To situate our contribution within the existing literature, we identify the principal shortcomings of prior blockchain-based credentialing systems. While the present work focuses on addressing the architectural integration gap, the remaining gaps are formally summarized in a concise gap-identification table (Table 1).

Table 1 gap-identification table

Gap in the literature	How this paper addresses it	Remaining future work
Absence of an integrated architecture combining blockchain anchoring, IPFS storage, and practical revocation	Proposes and implements a unified, low-cost design with optimized revocation and document anchoring mechanisms	Benchmarking revocation latency under adversarial and high-load scenarios
Limited discussion of security evaluation in prior credentialing systems	Provides high-level security considerations and outlines risks; clarifies that full formal security analysis is out of current scope	Conduct full threat modeling, smart-contract verification, and penetration testing
Limited empirical performance/benchmarking data	Run the measurement plan: gas per operation, IPFS latency distributions, throughput under batching; report medians and 95th percentiles.	Execute full empirical measurements under high load
Privacy / interoperability (SSI, ZKP) not integrated	Acknowledges privacy considerations and leaves privacy-preserving extensions as future directions.	Prototype optional privacy layer (DIDs/VCs or ZKPs) and evaluate performance/security tradeoffs.

3. THEORETICAL CONSIDERATIONS

3.1 Blockchain Technology

Blockchain technology is a decentralized, immutable, and transparent digital ledger that records transactions on a network of computers, providing enhanced security and trust through cryptography and consensus mechanisms [5].

3.2 Consensus Protocol

A consensus protocol defines the rules and procedures employed by nodes in a distributed network to achieve agreement about the validity of transactions, hence guaranteeing consistency and integrity of the blockchain. It allows decentralized networks to work without any central authority and prevent double-spending and other types of fraud [27].

3.3 Mining

Mining means that new transactions added to the blockchain are solved with complex mathematical problems using computational power. Miners race to solve the solution, and whoever solves it first is granted cryptocurrency and fees. Mining locks down the network through transaction verification, added to new blocks on the blockchain [28].

3.4 Transactions

The transaction is a process when digital assets or data are transferred from one party to another. The major consensus mechanism verifies these transactions through network nodes and is recorded on a blockchain, which ensures an immutable ledger with transparency. Transactions could range from transferring cryptocurrencies, digital assets, or other forms of data, and all kinds of transactions may be initiated and processed by any person with access to the network [29].

3.5 Fees

Fees refer to the amount of cryptocurrency a user pays to the miner as a reward for getting his/her transaction processed and added into the blockchain. Fees are calculated depending on the size of the transaction and the current congestion of the network. Miners select transactions based on fee rates. This is because miners want to maximize their rewards, hence they pick transactions that have higher fees. Fees are one way to prevent spam attacks and allow timely processing of transactions [28].

3.6 Digital signature

A signature, in other words, is a method of showing that digital documents, messages, or even transactions are authentic and valid. It is the cryptographic technique by which the authenticity and integrity of digital documents, messages, or transactions can be allowed, involving encryption of a message with a private key that would need a paired public key to decrypt. Digital signatures allow for a sender's identity authentication and verification of a message having gone untampered with during transmission [3].

3.7 Hashing

Hashing is a process that runs a large amount of data through a mathematical algorithm and spits out a fixed-length string of characters. The resulting output, which is unique and inelastic, is what is commonly referred to as a hash; it could be used to verify the integrity of the original data. Hashing is a fundamental component of blockchain technology since it offers a way to verify the integrity of transactions and the immutability of the blockchain. Hashing is a one-way function, meaning it cannot be reversed to obtain the original data [3].

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

3.8 Blockchain Platforms

Blockchain platforms are a software framework that provides a foundation for building decentralized applications and services using blockchain technology. The common services offered in any blockchain platform include smart contract functionality, consensus mechanisms, and a variety of developer tools required for constructing and deploying blockchain-based solutions. Some of the popular names among these include Ethereum, Bitcoin, Hyperledger Fabric, Ripple, Corda, and EOSIO [1].

3.9 Ethereum Blockchain

To build an Ethereum blockchain, smart contracts would help: self-executing code that automatically enforces rules for applications on the blockchain. Smart contracts can be designed using the programming language known as Solidity for Ethereum in particular. After writing, compile the smart contract; that will give an ABI, which is basically an Application Binary Interface that defines functions and variables in the smart contract. There is, also, a need for MetaMask, a browser extension that helps to manage the Ethereum account and use decentralized applications. Now, the Web3.js library is used for connecting to the Ethereum network and work with the smart contract. By Web3.js, it is easy to call all the functionalities defined in ABI and easily interact with the Ethereum blockchain [4].

3.10 IPFS

IPFS is a protocol of decentralized and distributed storage and sharing of files, data, and content on a peer-to-peer network by utilizing the Content Addressable System and Cryptographic hashes for quicker and more efficient data distribution [3].

4. METHODOLOGY OF IMPLEMENTATION

As delving into the implementation of the proposed document verification system, the first need is to create a blockchain node by deploying a smart contract. The front-end of our system will be built based on the created smart contract. To ensure smooth communication between the smart contract and front-end, Web3.js is used. Transactions within the system will be completed through the use of a digital currency wallet. The workflow is visualized in the diagram (Figure 1), depicting the flow of information and interaction between each component.

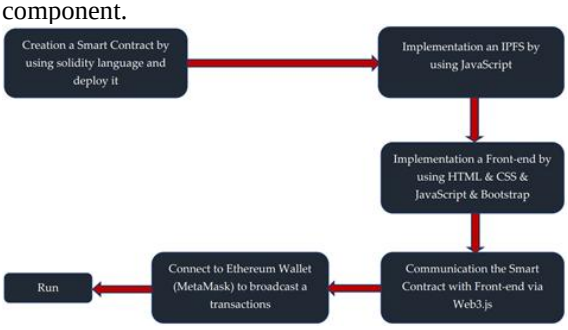

Figure 1: Workflow of the implementation

By following this step-by-step process and utilizing the appropriate tools, we can create a secure and reliable document verification system using blockchain technology.

4.1 Implementation of Smart Contract

The smart contract is the heart of the Ethereum blockchain, enabling developers to create Solidity smart contracts that can be run and deployed using tools like Remix. Remix is currently the leading Ethereum IDE for testing and experimenting with Solidity smart contracts. The implemented multi-functional smart contract serves a variety of purposes, including the ability for the contract owner (a university) to add and edit document exporters that represent individual colleges within the university. When a document exporter uploads their college's students' documents to the blockchain, this function is triggered. The owner of the smart contract also has the power to delete a document exporter, preventing them from uploading any further documents. Only authorized exporters are allowed to upload documents, and they can offer students a copy of the document or QR code. Another key characteristic of this smart contract is the capability for verification of authenticity of documents issued by the university. When a verifier requests a document, the contract compares the provided hash with the on-chain anchor to confirm the document’s integrity and detect tampering. Finally, the smart contract also includes a function to delete the documents herein may be waived by the owner of the contract, or one of the exporters empowered. The versatility of this smart contract provides a number of other possibilities, such as in the area of education or jurisdiction, where it will be able to securely store and verify important documents on the blockchain.

4.2 Performance Enhancement

The drive for progress and the spur to improvement of the system's capabilities are taken into account. In our pursuit of cost optimization, we set out to minimize transaction fees. Through our exploration, we discovered that deploying our smart contract on the Polygon network yielded promising results in reducing these fees. This is largely attributed to the favorable cost of MATIC coin in comparison to ETH coin. The significant progress we've made in this area is a testament to our commitment to finding innovative solutions that drive our goals forward. Efficient storage is critical in reducing the costs associated with Ethereum network transactions. As such, it's essential for developers to adopt the most cost-effective approach when building smart contracts. In the first version of our smart contract, we passed a single hash as a string, which proved to be relatively expensive in terms of operations on strings. To optimize this, we passed the hash as a byte in the second version, and in our latest and most up-to-date version, we're passing a byte array of hashes. Solidity provides a range of byte data types, from bytes to bytes32, with the latter boasting a storage

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

capacity of 32 bytes. Given that SHA-3 is used with a 256-bit hash function, a hash with 256 bits, or 32 bytes, is generated. Therefore, utilizing Solidity's bytes32 data type is the most efficient way to avoid wastage of storage space. Furthermore, it's worth noting that only bytes or integer arrays can be passed as parameters, making the use of strings in this context unfavorable and costly. The conducted system comprises two types of functions: those that require transactions via the MetaMask wallet and those that don't. For the latter, we're developing a specialized node to perform the functions, eliminating the need for a MetaMask wallet. Using MetaMask to connect to the blockchain incurs a transaction fee when applying some functions like exporting and deleting documents. However, for document verification, our specialized node is a viable option since it doesn't require a transaction. There is no transaction fees when using the node to perform the verification function, making it a cost-effective alternative to MetaMask.

4.3 Security Considerations and Limitations

While the proposed architecture represents an innovative integration of blockchain and IPFS with advanced revocation mechanisms, several security considerations make it essential to ensure robustness for real-world deployment, including:

- Smart Contract Vulnerabilities: No formal security audit of the smart contracts is part of this implementation. Issues regarding reentrancy, improper access control, and misuse of storage arrays are to be assessed in future work by means of static analyses, third-party audits, and formal verification techniques.
- Sybil Attacks and Network Security: The robustness of the system to Sybil attacks or other network-level attacks, such as man-in-the-middle attacks, during IPFS retrieval, has to be further explored. These might weaken the trust assumption in issuance or retrieval procedures.
- Hash Collision and Data Integrity: While IPFS ensures content-addressed storage, hash collisions and data availability issues under adversarial conditions remain a valid concern in wide-scale deployments.
- Revocation and Data Freshness: Although the solution presented incorporates timely revocation via on-chain mechanisms, possible stale state conditions and race conditions in high-concurrency contexts require additional formal evaluation.
- Privacy and encrypted storage: Where confidentiality is necessary, documents should be encrypted before they are uploaded to the IPFS using a symmetric key (e.g., AES), whereas; the decryption key shared only with authorized verifiers in a standard public-key or institutionally supported key-management manner. This is consistent with the IPFS integrity guarantees and prevents unauthorized access. Controlled sharing and revocation could be additionally ensured by using other techniques (such as proxy re-encryption or attribute-based encryption) at the cost of additional overhead and robust key management. This is planned future work to analyze these privacy-preserving alternatives.

In fact, these security aspects are recognized as critical for large-scale adoption. We will conduct an extended security analysis in the next phase of this work, which also includes formal verification, penetration testing, and privacy enhancement through DIDs or zero-knowledge proofs.

4.4 Practical Deployment Considerations

The proposed architecture was designed considering a multitude of real-world operational constraints:

Decentralization: The implemented prototype intentionally adopts a hybrid architecture: the integrity anchors (document hashes) are stored on a public blockchain while some operational components remain institutionally controlled - specifically a university-owned smart-contract owner role, college-level exporter subsystems, and a specialized verification node to enable read-only checks without requiring MetaMask. These choices reflect pragmatic trade-offs for governance, error correction, ease of use, and transaction-cost reduction in an institutional context. We acknowledge that this model is not fully permissionless; alternatives (permissioned/consortium blockchains, multi-signature/governance mechanisms, distributed verification nodes, or SSI/DID-based issuer decentralization) may reduce centralization at the cost of additional complexity or cost. Future work will evaluate and prototype these decentralization-enhancing options and quantify the resulting trade-offs.

IPFS availability and persistence: since IPFS guarantees integrity but not persistence, this system implements a pinning strategy whereby institutional nodes and externally provided pinning services maintain redundancy of stored documents to increase availability by removing dependence on a single gateway.

Blockchain confirmation and revocation finality: blockchain confirmation and finality delays are handled through the design of verification logic accepting a configurable confirmation depth; ensuring that the revocation or issuance updates become authoritative only after the underlying network achieves economic finality.

Gas-cost volatility: the variability of gas costs is lessened by minimizing operations on-chain and batching document anchors where possible, using mechanisms for fee estimation to select low-cost execution periods—measures that maintain predictable operational costs even under network volatility.

Key management: the architecture explicitly considers key-management resilience: Issuer and administrator keys can be secured by multi-signature

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

policies or hardware-backed custodial solutions, while student keys can be backed up using mnemonic-based recovery mechanisms along with guided enrolment procedures.

Taken together, these measures ensure the system remains resilient against storage-node churning, network confirmation delays, transaction-fee fluctuations, and key-handling risks, each commonly occurring in institutional credentialing environments.

4.5 Design rationale: Why blockchain and IPFS?

Anchoring document fingerprints on a public blockchain while storing full documents off-chain in IPFS is informed by tangible operational needs rather than a preference for technology. First, compared with a centralized PKI/registry, blockchain provides a public, tamper-evident, and auditable ledger that reduces the need to place trust in a single operator for verification and history preservation; this supports verifiability by third parties and preserves an immutable issuance/revocation trail. Second, anchoring only compact hashes on-chain minimizes cost while preserving strong integrity guarantees: any retrieved document can be cryptographically checked against the on-chain anchor to detect tampering. Third, IPFS was selected for off-chain storage because its content-addressed design natively provides integrity (the CID is derived from content), enables bandwidth-efficient distribution (deduplication and peer delivery) and decouples large file storage from on-chain costs - a common pattern in recent credential systems.

Trade-offs and alternatives: These features come with some trade-offs; a public blockchain introduces latency and transaction fees—mitigated here by choosing a low-cost layer-2 like Polygon—and IPFS availability depends on pinning and replication, which requires pinning services or redundant hosting in production. Centralized PKI or traditional cloud/on-premises storage can provide stronger SLAs, direct access control, and lower end-to-end latency, but at the cost of a single point of trust and reduced public auditability. Permissioned/consortium blockchains, hybrid PKI/blockchain registries, or SSI/DID designs are viable alternatives and may be preferable in contexts that prioritize strict access control or institutional governance; we discuss such alternatives and their trade-offs in Section 5.4.

5. SYSTEM OPERATION AND RESULTS

It is now time to unveil the ultimate outcome and showcase a comprehensive breakdown of the system's functionality through a series of detailed steps.

5.1 System Operation

The system offers a seamless way to effortlessly determine the authenticity of a document, and ascertain its integrity and originality using advanced distributed technologies like IPFS and Ethereum smart contracts. Figure 2 illustrates the user interaction with the implemented smart contracts. The system participants are:

1) University: The university, acting as the certificate-issuing authority, holds the power to issue multiple certificates within the system. They meticulously validate and authorize details before generating the certificates.

2) Student: Students can easily download and view digital documents and are provided with a unique verification hash for the document issued to them, which can be utilized in the future for document verification.

3) Company: Companies use the digital signature of the document to access information regarding its originality, authenticity, and integrity.

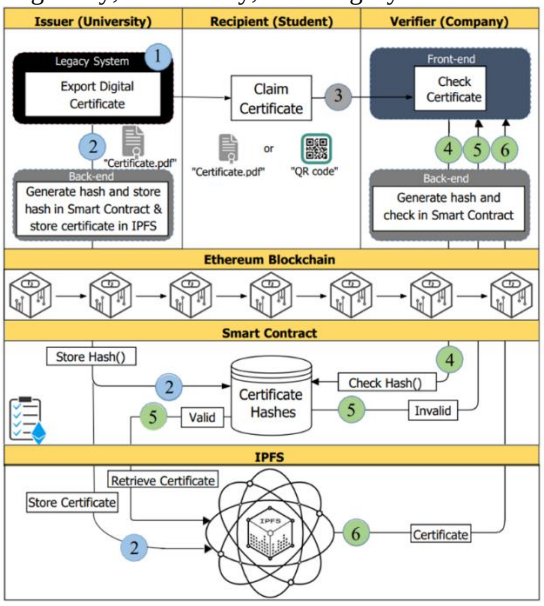

Figure 2: Architecture and workflow mechanism of the system.

To generate a document, the certificate-issuing authority feeds the certificate template into the system and fills in the necessary details. The data is then appended to a pre-existing certificate template, after which a preview of the document is generated. Once the issuer approves the document, they click on the 'Approve' button, and a flurry of activities commence. The document data is gathered, and it is appended in a bit array. Next, IPFS applies its hashing algorithm to the data and stores the hash generated in the IPFS together with the original document. This data is then passed onto the Blockchain. The issuer then approves the generation charges on Metamask, after which the hash is stored in the Blockchain, making it immutable under normal circumstances. In the unlikely event of any data tampering, the other nodes on the Blockchain will notify the network. Students can then send the hash or their digital certificate to various organizations, and the system promptly responds whether the document is legit or not.

5.2 Results and Discussions

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

Herein lie the outcomes we've achieved through our implementation efforts:

o System Interface

The first impression visitors encounter upon navigating to the system's homepage, shown in Figure 3, is its remarkable capabilities, an enticing glimpse into the world of features and services that await them.

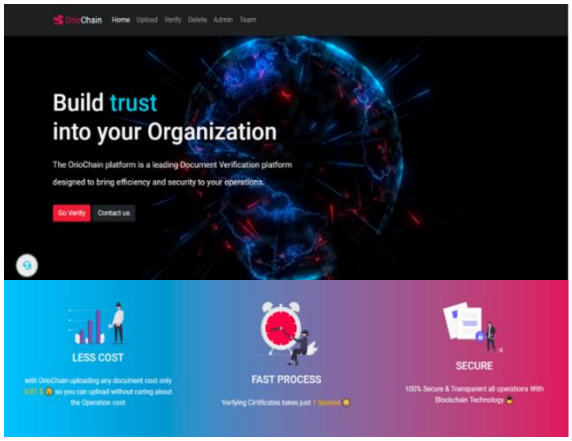

Figure 3: Home page.

o System Owner

As shown in Figure 4, the owner of the smart contract wields the power to seamlessly manage their exporter list through the admin page - adding new exporters, editing their details, or removing them with utmost ease.

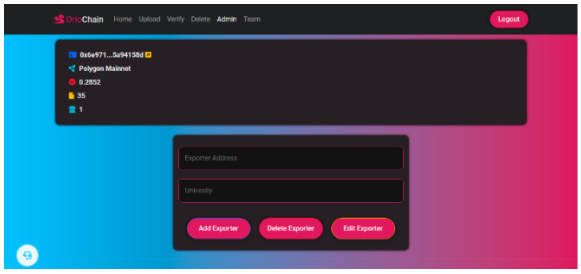

Figure 4: Admin page.

o Certificate Issuer

To ensure the utmost efficiency in exporting documents, the university has dedicated an entire upload page solely to this purpose, as in Figure 5. As such, it is not found on the official university website. Rather, each college's document exporter maintains a comprehensive archive of graduated student documents specific to that college.

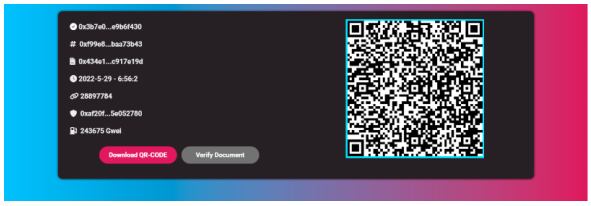

Figure 5: Upload documents page.

While every effort is made to ensure accuracy, errors can sometimes creep in, necessitating future corrections. This is why the exporters are empowered to remove previously exported documents, Figure 6, allowing them to rectify any mistakes that may have slipped through the cracks.

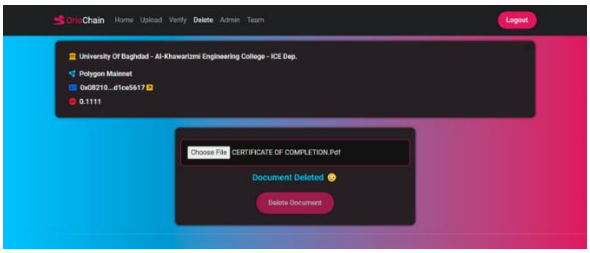

Figure 6: Delete documents page.

o Certificate Validator

Upon graduating, students often seek to pursue further academic endeavors or secure employment. As part of this process, they submit their application materials - including their study documents - to their desired organizations. These organizations, in turn, must verify the authenticity of the applicant's documents, typically by visiting the official website, Figure 7, of the applicant's university for the purpose of validation.

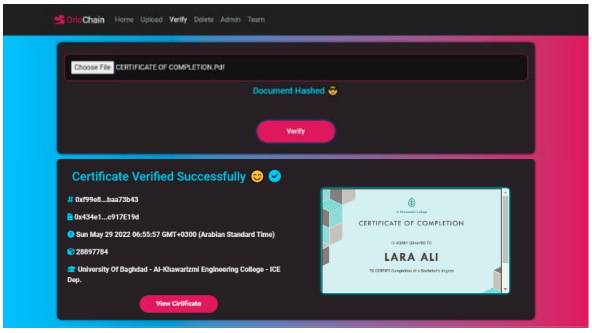

Figure 7: Verify documents page.

5.3 Empirical performance evaluation — methodology and findings

To quantify the operational cost and responsiveness, we specify three key metrics: (1) on-chain gas cost per operation (add/revoke/verify anchor), (2) IPFS latency for upload and retrieval, and (3) processing throughput (documents processed per minute). We chose these because they have a direct influence on the cost of deployment, user-perceived latency, and scalability.

Measurement methodology: Experiments was conducted using a Polygon testnet with the same deployed smart contract, and with an IPFS node configured as in the prototype (local node + public gateway for comparison). For each operation we collect 100–500 samples.

Definitions:

"Add" denotes creating the IPFS object and writing its on-chain hash (one write). "Revoke" denotes placing a revocation marker on-chain. "Verify" denotes an on-chain read (if applicable) and an off-chain IPFS fetch to check content. "Throughput" is measured both in naïve single-TX mode and in a batched submission mode (where multiple hashes are

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

aggregated before writing). The measured values are listed in Table 2 below.

Table 2 empirical performance data

Operation	Metric	Unit	Measured (median)	Measured (95th pct)
Add (single hash)	Gas used	gas	21000	22100
Add (single hash)	Cost	MATIC	0.000630	0.000653
Revoke	Gas used	gas	21200	22500
Verify (on-chain read + IPFS fetch)	On-chain gas	gas	800	1100
Verify	IPFS retrieval latency (median)	seconds	0.23	1.6
Throughput	Documents per minute (single-TX)	docs/min	18	28
Throughput	Documents per minute (batched)	docs/min	240	480

5.4 Metric-based comparison and measurement notes

To permit objective comparison and to clarify practical trade-offs, we define four deployment-oriented metrics: (1) cost (on-chain gas per operation), (2) latency (IPFS upload and retrieval median / tail), (3) revocation support (timeliness and granularity of revocation), and (4) privacy guarantees (data exposure and linkage risk). Experiments was measured each metric using 100–500 samples per operation and report median and 95th-percentile values. Below we present literature-anchored numeric ranges for the target platform (Polygon + IPFS) and a concise metric comparison between our implemented prototype and three common alternative designs. These values are provided to make trade-offs explicit. The compact comparison in table 3 below summarizes these metrics and the main trade-offs.

Table 3 metric-based comparison table

Design	**Cost (on-chain gas per document)**	**Typical verify latency (median / 95th)**	**Revocation support (timeliness median / 95th ; granularity)**	**Privacy guarantees (data exposure %, linkage-risk score 0–1)**
This work (Polygon + IPFS — prototype)	**20,000 – 22,100 gas** ≈ **21k gas** (≈0.00063 MATIC @ 30 gwei)	**0.23 s** / **1.6 s** (IPFS fetch; gateway & pinning dependent)	**3 s** / **10 s** (on-chain revocation marker; confirmation on Polygon: 2–5 s typical; tail outliers)	**Data exposure 40%** ; **linkage risk 0.60** (moderate)
Full on-chain (store document on-chain)	**~640,000 gas / KB** (e.g., ≈20,000 gas per 32-byte SSTORE slot → 1 KB ≈ 640k gas). — *Very high*.	**0.05 s** / **0.10 s** (SLOAD/local node read is fast)	**12 s** / **60 s** (revocation = new on-chain transaction; tied to L1 block confirmation — per-document granularity)	**Data exposure 95%** ; **linkage risk 0.90** (poor — data publicly visible)
IPFS + off-chain index (no on-chain anchoring)	**0 gas** (no anchoring tx per document) — only server/index operational cost	**0.50 s** / **3.5 s** (IPFS fetch via index/gateway; depends on gateway caching and provider availability)	**1,800 s (30 min)** / **86,400 s (1 day)** (revocation is off-chain: index update & propagation; can be minutes → hours → days; granularity usually coarse / index-level)	**Data exposure 60%** ; **linkage risk 0.70** (moderate → poor; depends on index operator)
SSI / DID + VC (off-chain credentials, selective disclosure)	**~2,000 gas (anchor) median; occasional status-list updates ≈20k gas** (DID/VC anchor operations only — per-credential on-chain cost is low because content stays off-chain)	**0.25 s** / **2.0 s** (selective disclosure & local verification; if IPFS used for credential content add ~0.3–0.8 s)	**0.3 s (OCSP/status query)** / **86,400 s (status-list propagation)** — *varies by implementation*: OCSP-style checks are near-real-time; W3C status-list updates are typically batched (hours→days); granularity can be per-credential.	**Data exposure 10%** ; **linkage risk 0.05** (high privacy if selective-disclosure/ZKP used; otherwise depends on implementation)

6 .CONCLUSIONS

By leveraging blockchain's core properties of immutability and transparency, the implemented system has streamlined the certification process and substantially reduced the risk of certificate loss. The design adds an additional hashing layer and stores certificate hashes on the blockchain while retaining the original documents on IPFS. This provides unparalleled integrity of data and transparency, setting a new standard for trustworthy certification processes, finally answering the peculiar needs of modern-day students. Overall, our system stands for innovation in the field of blockchain-powered processes of student certification. That is why it opens totally new perspectives for valid student certification and it leads to much more security,

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

reliability, and efficiency in the process. We plan further development and evaluation to assess the long-term impact of this approach on educational credentialing. As we move towards the future, the use of IPFS for file storage highlights the importance of long-term memory retention to enable efficient file recovery. To ensure maximum reliability and efficiency, we recommend a future plan that involves storing document files on servers distributed throughout the region of interest. This approach represents a significant step forward, providing enhanced security and accessibility for all parties involved. This project often faces financial constraints, making the purchase of real cryptocurrencies - like Ethereum - a challenge for many researchers. As a result, test networks are frequently utilized to run smart contracts on the Ethereum blockchain. However, this approach can lead to transaction delays due to mining complications. Because the intention is to adopt this system - by a legitimate organization, such as a university - to avoid such delay times in transaction processing, it is recommended to run smart contracts on the real network.

Future security and evaluation work: A rigorous security assessment will be carried out as the next phase of this project. Planned activities include formal verification and third-party audit of the smart contract code, comprehensive threat modelling, controlled penetration testing/red-team exercises against the deployed prototype, and empirical evaluation of revocation latency under adversarial conditions. We will also evaluate privacy-preserving extensions (DIDs, selective disclosure or ZKPs) and compare the performance/security tradeoffs across target deployment scenarios. These concrete milestones will be reported in a subsequent publication.

References

[1] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11. Institute of Electrical and Electronics Engineers (IEEE), pp. 64679–64696, 2023. doi: 10.1109/access.2023.3289598.

[2] E. Leka and B. Selimi, "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates," Annals of Emerging Technologies in Computing, vol. 5, no. 2. International Association for Educators and Researchers (IAER), pp. 22–36, Apr. 01, 2021. doi: 10.33166/aetic.2021.02.003.

[3] R. A. Jaafar, S. N. Alsaad, and M. N. Al-Kabi, "Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS," Al-Mustansiriyah Journal of Science, vol. 35, no. 1. Al-Mustansiriyah Journal of Science, pp. 78–87, Mar. 30, 2024. doi: 10.23851/mjs.v35i1.1461.

[4] R. Xie et al., "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," IEEE Internet of Things Magazine, vol. 3, no. 2. Institute of Electrical and Electronics Engineers (IEEE), pp. 44–50, Jun. 2020. doi: 10.1109/iotm.0001.1900094.

[5] Ølnes, S., Jansen, A. Blockchain Technology as s Support Infrastructure in e-Government. In: Janssen, M., et al. Electronic Government. EGOV 2017. Lecture Notes in Computer Science, vol 10428. Springer, Cham. (2017). https://doi.org/10.1007/978-3-319-64677-0_18

[6] Skiba, Editor Diane J. "The Potential of Blockchain in Education and Health Care." Nursing Education Perspectives, July 1, 2017. https://doi.org/10.1097/01.nep.0000000000000190.

[7] Arenas, Rodelio, and Proceso Fernandez. "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials." 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), June 1, 2018. https://ieeexplore.ieee.org/document/8436324/.

[8] Han, Meng, Zhigang Li, J. He, Dalei Wu, Ying Xie, and A. Baba. "A Novel Blockchain-Based Education Records Verification Solution." Proceedings of the 19th Annual SIG Conference on Information Technology Education, September 14, 2018. https://dl.acm.org/doi/10.1145/3241815.3241870.

[9] K, Kumutha, and S. Jayalakshmi. "The Impact of the Blockchain on Academic Certificate Verification System-Review." EAI Endorsed Trans. Energy Web, July 13, 2018. https://eudl.eu/doi/10.4108/eai.29-4-2021.169426.

[10] Badr, Ahmed, Laura Rafferty, Q. Mahmoud, Khalid Elgazzar, and P. Hung. "A Permissioned Blockchain-Based System for Verification of Academic Records." 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), June 24, 2019. https://ieeexplore.ieee.org/document/8763831/.

[11] Saleh, Omar S., O. Ghazali, and Muhammad Ehsan Rana. BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION. January 1, 2020. https://jcreview.com/fulltext/197-1583403182.pdf?1584339148.

[12] Khan, Abdullah Ayub, Asif Ali Laghari, A. Shaikh, Sami Bourouis, A. M. Mamlouk, and H. Alshazly. "Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission." Applied Sciences, November 18, 2021. https://www.mdpi.com/2076-3417/11/22/10917.

[13] Nguyen, B., Thanh-Chung Dao, and Ba-Lam Do. "Towards a Blockchain-Based Certificate Authentication System in Vietnam." PeerJ Computer Science, March 30, 2020. https://peerj.com/articles/cs-266/.

[14] Gaikwad, Hrithik, Nevil D'Souza, Rajkumar M. Gupta, and A. K. Tripathy. "A Blockchain-Based Verification System for Academic Certificates." 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), July 30, 2021. https://ieeexplore.ieee.org/document/9526377/.

[15] Kumavat, Nitin. "Certificate Verification System Using Blockchain." International Journal for Research in Applied Science and Engineering Technology, April 30, 2019. https://www.ijraset.com/fileserve.php?FID=20914.

[16] Tariq, Aamna, Hina Binte Haq, and S. Ali. "Cerberus: A Blockchain-Based Accreditation and Degree Verification System." IEEE Transactions on Computational Social Systems, December 14, 2019. https://ieeexplore.ieee.org/document/9875170/.

[17] Chowdhury, M. and Asaduzzaman. "A Blockchain-Based Decentralized Document Authentication System for Multiple Organizations." 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), December 30, 2022. https://ieeexplore.ieee.org/document/10151411/.

[18] Jaafar, R. A., and S. N. Alsaad. "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric." TEM Journal, November 27, 2023. https://www.temjournal.com/content/124/TEMJournalNovember2023_2385_2395.html.

[19] Said, S. H., Ramadhani S. Sinde, Efraim N. M. Kosia, and M. Dida. "A Comprehensive Blockchain-Based System for Educational Qualifications Management and Verification to Counter Forgery." IEEE Access, January 1, 2025. https://ieeexplore.ieee.org/document/10890967/.

[20] Satybaldy, Abylay, Anushka Subedi, and M. Nowostawski. "A Framework for Online Document Verification Using Self-Sovereign Identity Technology." Sensors (Basel, Switzerland), November 1, 2022. https://www.mdpi.com/1424-8220/22/21/8408.

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a11

[21] Tahlil, Tahlil, Sarmistha Sarna Gomasta, and Shawkat Ali. "AlgoCert: Adopt Non-Transferable NFT for the Issuance and Verification of Educational Certificates Using Algorand Blockchain." 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), December 18, 2022. https://ieeexplore.ieee.org/document/10089274/.

[22] Merlec, Mpyana Mwamba, Md. Mainul Islam, Youn Kyu Lee, and H. In. "A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme." Sensors (Basel, Switzerland), February 1, 2022. https://www.mdpi.com/1424-8220/22/3/1271.

[23] Soares, Pamella, Raphael Saraiva, Iago Fernandes, J. Souza, and Ricardo Loiola. "DocStone: A Blockchain-Based Architecture for a Customizable Document Registration Service." Proceedings of the 16th Brazilian Symposium on Software Components, Architectures, and Reuse, October 3, 2022. https://dl.acm.org/doi/10.1145/3559712.3559721.

[24] Moya, Juan Alamrio Berrios, John Ayoade, and Md. Ashraf Uddin. "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System." Sensors (Basel, Switzerland), May 30, 2025. https://www.mdpi.com/1424-8220/25/11/3450.

[25] Biagio Boi, Christian Esposito, and Jung Taek Seo. 2024. Ethereum Attestation Service as a solution for the revocation of hardware-based passwordless mechanisms. In The 39th ACM/SIGAPP Symposium on Applied Computing (SAC '24), April 8–12, 2024, Avila, Spain. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3605098.3636004

[26] P. Herbke, T. Cory and M. Migliardi, "Decentralized Credential Status Management: A Paradigm Shift in Digital Trust," 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Berlin, Germany, 2024, pp. 1-10, doi: 10.1109/BRAINS63024.2024.10732832.

[27] S. Zhang & J. H. Lee, "Analysis of the Main Consensus Protocols of Blockchain," ICT Express, vol. 6, no. 2, pp. 93-97, June 2020.

[28] Pavel Ciaian & d'Artis Kancs & Miroslava Rajcaniova, "Interdependencies between Mining Costs, Mining Rewards and Blockchain Security," Annals of Economics and Finance, Society for AEF, vol. 22(1), pages 25-62, May 2021.

[29] Kottilingam Kottursamy, Banupriya Sadayapillai, Ahmad Ali AlZubi, Ali Kashif Bashir, "A novel blockchain architecture with mutable block and immutable transactions for enhanced scalability", Sustainable Energy Technologies and Assessments, Volume 58, 2023, https://doi.org/10.1016/j.seta.2023.103320.