International Journal of Safety and Security Engineering
Vol. 15, No. 6, June, 2025, pp. 1185-1195
Journal homepage: http://iieta.org/journals/ijsse

A Hyperledger-Based Secure Framework for Academic Certificate Authentication Using Blockchain

Siba Prasad Dash[1], Ajay Kumar Jena[1*], Dileep Kumar Murala[2]

[1] School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar 751024, India
[2] Department of Computer Science and Engineering, Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad 501203, India

Corresponding Author Email: ajay.bbs.in@gmail.com

https://doi.org/10.18280/ijsse.150610

Received: 10 May 2025
Revised: 13 June 2025
Accepted: 24 June 2025
Available online: 30 June 2025

Keywords:
blockchain technology, certificate authentication system, Inter Planetary File System (IPFS), Hyperledger Fabric, authentication, decentralisation

ABSTRACT

Certificate authentication is often a tedious and complex process, particularly for critical documents such as academic degrees, which require rigorous verification to prevent fraud. Traditional methods are slow, prone to errors, and heavily reliant on manual effort, making it difficult to detect sophisticated counterfeit certificates that can undermine the credibility of both students and issuing institutions. To address these challenges, this study proposes and develops a blockchain-based Certification Verification System using Hyperledger Fabric. The system enables universities to issue and upload academic credentials to a secure, permissioned blockchain, ensuring the immutability, authenticity, and confidentiality of records. By decentralizing certificate storage, the platform allows only authorized parties to access and verify data, reducing processing time, enhancing transparency, and safeguarding against tampering. Hyperledger Fabric was selected for its privacy features, scalability, and enterprise-grade capabilities, eliminating the need for cryptocurrency while providing controlled access. Each participant is equipped with device-specific certificates for robust authentication, further reinforcing security. In this study, evaluation of Blockchain Platforms Based on TPS, Consensus, and Certificate Suitability using Hyperledger Fabrics outperform in the comparison with Ethherium and botcoin platforms. This integrated system empowers students to manage and share their verified credentials easily and allows employers to perform real-time, trustworthy verification. Overall, the study demonstrates that blockchain technology, when implemented through permissioned frameworks like Hyperledger Fabric, offers a reliable, future-ready solution for modernizing academic credential verification while upholding the principles of security, decentralization, and trust.

1. INTRODUCTION

A blockchain can be succinctly described as a sequential chain of interconnected information chunks. Blockchain technology has emerged as a prominent tool facilitating transparent, tamper-proof information sharing inside a network. It is an unalterable record-keeping system composed of several blocks for the storage of transactions/data. Each block generates a cryptographic hash of its header and transmits it to its subsequent block in the chain. The decentralized structure, wherein each block contains an identical copy of the ledger data, enables the nodes in the blockchain to observe real-time transactions occurring within the network. This facilitates transaction tracing and enhances transparency [1]. The robustness of blockchain technology arises from three fundamental features. (i) the distributed and decentralized architecture, (ii) the interconnection of blocks via cryptographic hashes derived from the preceding block's contents, and (iii) the immutability and challenge of modifications; as altering any block necessitates the alteration of all following blocks. The resilience and transparency render it an excellent option for diverse applications in finance, marketing, supply chain management, intellectual property protection, and voting systems [2].

Blockchain technology can be utilized to address the issue of counterfeit educational diplomas, a significant social concern. Counterfeit certifications may adversely affect equitable access to higher education programs. It can exert considerable adverse impacts on individuals, organizations, and society at large. The unnoticed acceptance of counterfeit certificates during the selection process undermines trust in educational institutions, certification authorities, and candidates possessing authentic degrees and achievements. The institution that neglects to authenticate qualifications may experience diminished credibility and reputational harm. Employing individuals based on counterfeit credentials can be exceedingly harmful to any organization. This may result in an inept workforce devoid of essential skills and competencies, ultimately diminishing productivity and job quality, so obstructing overall organizational progress. In critical sectors such as healthcare and aviation, public safety and security are of utmost importance, as inadequate employment practices can present substantial risks to life [3].

To alleviate the detrimental impacts of counterfeit certificates, institutions, employers, and certifying bodies must establish rigorous verification protocols that authenticate both the certificate issuer and the certificate itself. This work aims to offer a system for verifying certificates and their issuers. This paper presents a decentralized blockchain-based system for verifying the authenticity of certificates. It guarantees that every certificate issuer is a credible and reliable entity authorized to issue certificates. Current studies on blockchain-based certificate verification systems reveal effective methodologies for secure certificate issuance, verification, and rectification functionalities. There remains a necessity for a complete platform that enables many institutions to effortlessly issue and authenticate certificates inside a unified, safe environment. Current research predominantly emphasizes singular institutions and is deficient in inter-institutional functionality. To meet this need, this paper suggests a decentralised blockchain-based system for securely issuing and checking educational certifications. The system makes sure that only allowed and trustworthy organisations can issue certificates. It also makes sure that any stakeholder may independently verify these credentials without having to rely on central authorities. A lot of research has been done on how to use blockchain for certificate administration, but most of it is about solutions that work for a single institution or a small number of use cases. These implementations usually don't work with other systems, don't allow collaboration between institutions, and often need trusted third parties to check or control them. On the other hand, the proposed architecture creates a single, scalable platform that lets several institutions issue and verify certificates without any problems in a decentralised setting. This system is better than current ones since it doesn't need central middlemen and lets institutions work together. It is also more stable, flexible, and open. It offers dynamic registration of certificate issuers, secure validation across institutions, and scalable adoption for real-world deployment, making it well-suited for global academic and professional ecosystems.

1.1 Contribution

- ➢ This paper presents a blockchain-based decentralised, and trusted certificate authentication system, wherein certificates issued by a trusted authority are validated through smart contract code on a permissioned blockchain.
- ➢ We provide an innovative method for safe certificate updates and revocation within a blockchain-based certificate authentication system, featuring access restriction restricted just to authorised issuers.
- ➢ We implement an Application Programming Interface (API) to facilitate the seamless integration of the suggested solution with the existing system.
- ➢ We offer a consolidated platform for certificate authentication that facilitates the issuing and verification of certificates from many institutions inside a singular secure ecosystem.

2. LITERATURE SURVEY

Educational certificates serve as a significant indicator of proficiency and must be shown as evidence when seeking higher education or employment. Due to the significance of these credentials, some counterfeit documents have been detected [1]. Various methods, like as stamps, holograms, and wet signatures, have been utilised to tackle this issue; nevertheless, these can be easily replicated and may facilitate the creation of counterfeit documents. Current studies and use of blockchain technology across several domains have demonstrated enhanced security and reliability [1]. Blockchain functions as a unified platform for data exchange, storage, and document access, thereby diminishing the time needed for certificate verification [2]. A distributed application was built to store user identities by integrating national identity numbers with blockchain technology, so obviating the necessity for individuals to carry physical ID cards at all times [3]. Reference [4] the application necessitates user participation, which can be validated by Blockchain technology. A blockchain can document a user's governmental identification and biometric data. Upon accessing a user's ID, a transaction is initiated for documentation purposes. The integration of biometrics and blockchain enhances the system's overall security [5]. Employers need not reach out to the certificate issuer for the validation of educational credentials; rather, smart contracts can facilitate the comparison of the hash of submitted certificates against the hashes stored on the blockchain. IPFS enables the creation of a secure lifelong educational portfolio [6]. Educational qualifications on a blockchain must adhere to particular security principles, as outlined in the study [7]:

1. Authentication: All users must be authorised. Students, institutes, universities, and other entities may use this service [8].
2. Authorisation: Users are granted authority to conduct transactions on the blockchain. For example, once the certificate has been issued by the issuer, the student will have full control over it [9].
3. Confidentiality: The academic establishment must safeguard the student's private information [10].
4. Ownership: The blockchain ledger's users determine who owns a digital certificate.
5. Privacy: Public keys are stored anonymously [11].

The topics stated above are critical in determining whether or not a certificate is fraudulent. Numerous implementations have previously been offered. KMI, OU - UK pioneered the use of blockchain as a trusted ledger to manage web reputation, badges, and certificates. The primary emphasis was on creating blockchains for higher education qualifications in the UK [12]. Confidential data was disclosed on a public blockchain, presenting a risk. No method existed to safeguard the recipient's ownership and privacy. This implementation encountered some difficulties [13]. The University of Nicosia utilised bitcoins for multiple purposes. Educational certificates in blockchain technology were established to mitigate fraud. They provided software tools that enabled users to authenticate the certificate's validity. The SHA-256 hashing algorithm is employed for the distribution of certificates in PDF format. The disadvantages encompass the absence of a definitive method for validating the validity of parties [14]. The application of hash values was also endorsed in the study [15], where the hash value was calculated for both document enrolment and authentication. The MIT Media Lab has implemented Blockcerts for the creation of digital certificates. The issuer initially generates the digital certificate, after which the hash is incorporated into the blockchain transaction. The recipient of the certificate is then allocated the output of the transaction. This implementation presents issues with ownership and privacy [16]. The degree of trust is inadequate. All individuals had access to the certificates. The certifications stored on the blockchain are immutable, although they can be falsified. Security and privacy are supplementary concerns in this implementation.

SmartCert [17] is an additional blockchain-based solution for the verification of digital credentials. It is intended to tackle the problem of counterfeit certifications. This system is susceptible to attack. Educational institutions can employ RecordKeeper to issue certificates and provide users with a receipt, which can subsequently be shared with a third party to verify the certificate's authenticity [18]. This method has several difficulties; however, those seeking to access the RecordKeeper blockchain's certificate must possess ownership rights. This results in a danger of tampering, which may occur due to the transfer of ownership to a third party. This technique is more appropriate for a private blockchain as it guarantees the security of the certificate [19]. There are various methods to store the certificates. A database can be established to document certificates, allowing for their revocation, with the revocation status likewise recorded on the blockchain, so ensuring transparency due to its intrinsic append-only characteristic [20]. This study advocates for the utilisation of blockchain technology to authenticate both students and the certificates issued to them, eliminating the need for a third party [21]. It is executed on Ethereum, an open-source platform and public blockchain [22]. Furthermore, it is necessary to correlate student identification with the issued certificate, which is also executed in this endeavour. Researchers have been looking for ways to improve security and interoperability since 2022. For instance, reference [23] suggested a digital diploma system based on blockchain that includes self-sovereign identification (SSI). This gives users more power while keeping the data safe. In paper [24] came up with a hybrid blockchain architecture that combines Hyperledger Fabric with Ethereum. This makes it possible to handle private data and verify it in public. One of the main problems with immutable ledgers in education is that they don't allow for revocation or dynamic modifications. Their method does. Singh et al. [25] looked into using zero-knowledge proofs (ZKPs) to check academic credentials without giving up private information. This would make public verification systems better at protecting privacy. In article [26] created a role-based access control system with smart contracts. On the blockchain, issuing authorities, students, and verifiers all have different permissions. This architecture protects against unauthorised access and keeps the integrity of the certificate throughout its life.

Even with these improvements, many current implementations either don't have full inter-institutional support or use broken frameworks that don't operate with more than one issuing authority [27-32]. They also don't always provide smooth, end-to-end solutions that strike a compromise between privacy and openness. This work, on the other hand, tries to fill up these holes by suggesting a decentralised blockchain-based system that allows several institutions to operate together, requires strong issuer authentication, and protects user privacy and ownership [33]. The system uses smart contracts to automate tasks, IPFS for off-chain storage, and public-key cryptography for safe access. This makes it a complete, scalable solution that gets beyond the problems with previous initiatives.

3. PROPOSED APPROACH

This paper suggests a secure and verifiable system for digitising certificates based on Hyperledger Fabric, a private, permissioned blockchain infrastructure that works well for consortium-based deployments. The system makes sure that all transactions associated to certificates are permanent, traceable, and private, while also making it easier for only approved companies to regulate access and keep data safe.

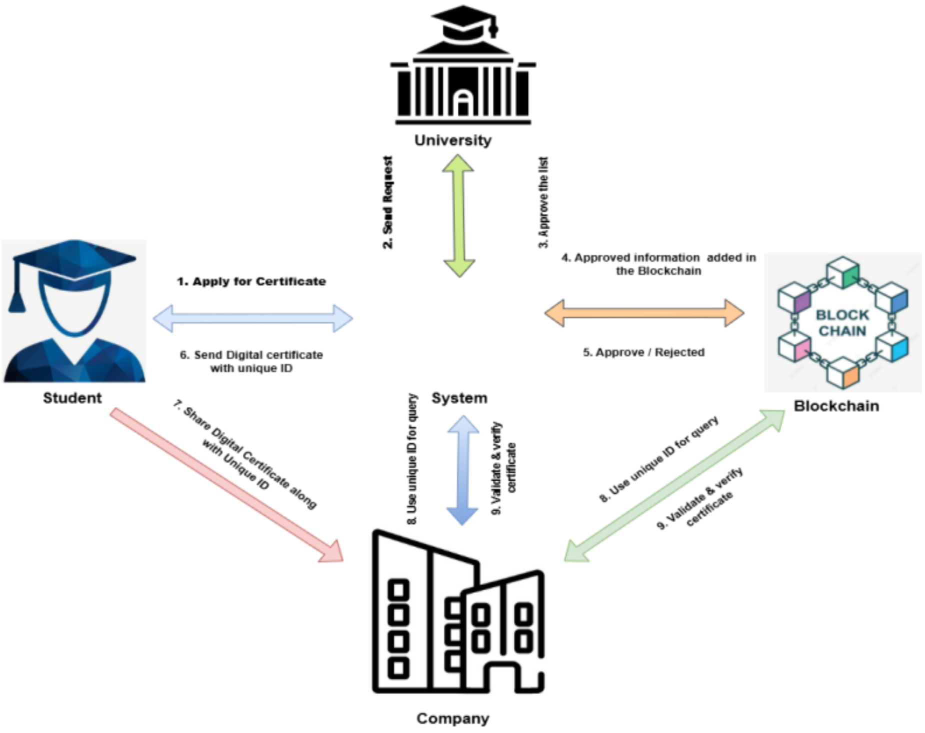

University
2. Send Request
3. Approve the list
1. Apply for Certificate
4. Approved information added in the Blockchain
BLOCK CHAIN
6. Send Digital certificate with unique ID
5. Approve / Rejected
Student
System
Blockchain
7. Share Digital Certificate along with Unique ID
8. Use unique ID for query
9. Validate & verify certificate
8. Use unique ID for query
9. Validate & verify certificate
Company

Figure 1. Flow diagram of certificate verification system

3.1 System architecture

As shown in Figure 1, the system consists of the following key components:

System Administrator: Responsible for configuring the blockchain network, defining smart contract logic (chaincode), registering institutions, and managing certificate issuance privileges.

Certificate Issuers (Institutions): Entities authorised to issue certificates. Each issuer must be registered and assigned a digital identity (X.509 certificate) by the Certification Authority (CA).

End Users (Students and Verifiers): Students are issued certificates and have ownership privileges, while verifiers (e.g., employers, academic institutions) can validate certificate authenticity via public access or consented sharing.

3.2 Smart contract (chaincode) logic

Smart contracts, also known as chaincode in Hyperledger, define the business logic that governs how certificates are issued, updated, verified, and accessed. Key smart contract functions include:

CreateCertificate (assetID, issuerID, studentID, metadata): Validates issuer permissions and creates a certificate asset with a unique assetID. The metadata includes certificate type, issue date, program details, and IPFS hash for the PDF file.

UpdateCertificate (assetID, updatedMetadata): Allows certificate corrections by authorised issuers. The updated data is appended as a new version linked to the original assetID.

RevokeCertificate (assetID): Revokes an existing certificate and logs the reason for revocation.

VerifyCertificate (assetID): Fetches current metadata for the specified assetID and returns its cryptographic hash for verification purposes.

LogAccess (assetID, viewerID, timestamp): Automatically logs access requests to a certificate, creating a transparent view history.

All transactions are recorded in a ledger with corresponding timestamps and digital signatures to ensure non-repudiation and integrity.

3.3 Data storage structure

The system uses a key-value store (LevelDB or CouchDB) embedded in Hyperledger Fabric’s state database to store certificate data. The structure is as follows:

Key: Unique assetID (e.g., CERT12345)

Value: JSON object containing:

•issuerID

•studentID

•issueDate

•programDetails

•certificateHash (hash of PDF stored on IPFS)

•status (active, revoked)

•versionHistory (array of metadata changes)

•accessLog (array of viewerIDs and timestamps)

To ensure scalability and efficient retrieval, a composite key is generated using asset type and asset ID (e.g., certificate~CERT12345) for indexed queries.

3.4 Access control mechanisms

Access control is enforced through Hyperledger Fabric’s Membership Service Provider (MSP) and Attribute-Based Access Control (ABAC). The roles and their permissions are defined in the chaincode and the accessControl.yaml configuration:

Admin: Full access to all smart contract functions.

Institution: Can issue, update, and revoke certificates it owns.

Student: Read-only access to their own certificates; can grant access tokens to third parties.

Verifier: Can verify certificates only if granted a token by the student or if certificate is publicly marked.

Smart contracts check user credentials and attributes before executing any transaction, ensuring granular permission control.

3.5 IPFS integration

The certificate PDF files are stored off-chain using the InterPlanetary File System (IPFS). The hash of each file is stored on-chain, enabling verifiers to:

•Retrieve the file from IPFS using the hash.

•Validate the integrity by re-hashing the file and comparing it to the stored hash.

This hybrid storage model ensures that the blockchain remains lightweight and scalable while maintaining the benefits of decentralised file storage.

3.6 Transaction immutability and auditability

Each transaction certificate issuance, update, revocation, and viewing is recorded as a block entry. The Hyperledger ledger maintains both the current state and full transaction history (world state and blockchain log), ensuring all operations are traceable. Any modification results in a new state while preserving the history for audit purposes.

Unauthorized access attempts or view requests are recorded using the LogAccess function, enabling forensic audits and detection of suspicious behaviour.

4. IMPLEMENTATION

This technology effectively deploys a Hyperledger-based private blockchain. Each asset documented on the blockchain produces a uniquely identifiable hash. If the hash is altered, it will no longer correspond to the original. Thus, it is very impossible to alter anything. Information creation and change will be documented as transactions. Figure 1 illustrates the comprehensive architecture of the system, which is detailed below:

The Figure 1 shows a Hyperledger Fabric-based Blockchain-Based Certificate Authentication System conceptual architecture. This system secures, authenticates, and tracks institution-issued academic and professional certifications. The architecture has four main components: the Student, the Institution (such a university), the Blockchain (Hyperledger Fabric), and the Web Application providing the user interface and service bridge. Blockchain, an immutable ledger, stores critical certificate information such certificate ID, issue date, issuing authority, and a digital hash of the certificate file. This immutable storage ensures that a certificate cannot be changed without discovery. The Hyperledger Fabric platform allows only authorised organisations to write data to a permissioned blockchain, improving data governance and privacy. Certificates are issued by the trustworthy Institution. Institutions upload certificate details to the Web Application after students complete programs or training. These details are hashed and transferred to the blockchain via smart contracts. The university must also handle student requests for changes or re-issuance, which may result in a new blockchain certificate entry with the previous marked as superseded.

Web Application is the main way students use the system. They can log in, upload certificates, examine certificate history, and request verification. To confirm a certificate's legitimacy to an employer, a student or verifier can enter the certificate ID or upload the file to the online application. The system compares the uploaded document hash to the blockchain hash. If they match, the certificate is legitimate and unchanged. The Web Application connects students and institutions to the blockchain network. It controls user sessions, smart contracts, certificate uploads, and verification outcomes. This centralised interface streamlines blockchain interactions and hides the complexity from end-users while preserving blockchain's decentralisation. This architecture makes certificate administration robust, transparent, and tamper-resistant. It eliminates forgeries, creates trust in academic and professional credentials, and speeds up and improves verification for all stakeholders. The logical flow of our approach can be described by a variety of parameters. These equations and relationships formalise the operations that our system represents, such as smart contract issuance, storage, verification, authentication, and execution.

1. Credential issuance: This explains how a university U_j provides a certification C_i to a student S_i. The credential includes crucial information such as the degree, year, and student ID, and it is digitally authenticated by the university to ensure its authenticity. The signed credential is bundled into a block B_i with a reference to the preceding block's hash to ensure blockchain continuity and tamper protection.

$$C_i = \{\, \mathrm{Data}(S_i), \mathrm{Degree}, \mathrm{Year}, \ldots \} \qquad (1)$$

$$B_i = \mathrm{Block}(C_i, \mathrm{Sig}_{uj}(C_i), \mathrm{PrevHash}) \qquad (2)$$

Algorithm 1: Create Certificate

```
CreateCertificate(studentName, course, issuer, issueDate, fileHash)
1. Verify certID in ledger.
2. If exists, return "Certificate already exists."
3. Create certificate object:
{{certID: certID, studentName: studentName, course: course, issuer: issuer, issueDate: issueDate, fileHash: fileHash, status: "active", correctedFrom: null}
4. Put the certificate object in the ledger with certID as the key.
5. Report "Certificate created successfully."
```

2. Verification Request: When an employer or enterprise E_k needs to verify a student's credential C_i, the system verifies if the credential and digital signature exist and match the blockchain record. The result V_{ik} delivers 1 for legitimate credentials and 0 for false or altered credentials, offering a trustworthy and real-time verification process.

$$V_{ik} = \mathrm{Verify}(C_i, \mathrm{Sig}_{uj}(C_i), B) \qquad (3)$$

Algorithm 2: Verify Certificate

```
VerifyCertificate(certID, inputHash)
1. Use certID to get the ledger certificate.
2. Error: "Certificate not found."
3. Check inputHash against fileHash.
4. If match:
Returned: "✓ Valid certificate."
Else:
Returned:"❌ Certificate is invalid or has been tampered."
```

3. Access Control and Authentication: This technique ensures that only authorised users (students, universities, and employers) have access to the system. The system verifies each user's device-specific certificate (Cert_x) before enabling operations. This prevents unauthorised access and spoofing attacks. if $\mathrm{Verify}(\mathrm{Cert}_x) = 1$ it returns true, otherwise return False.

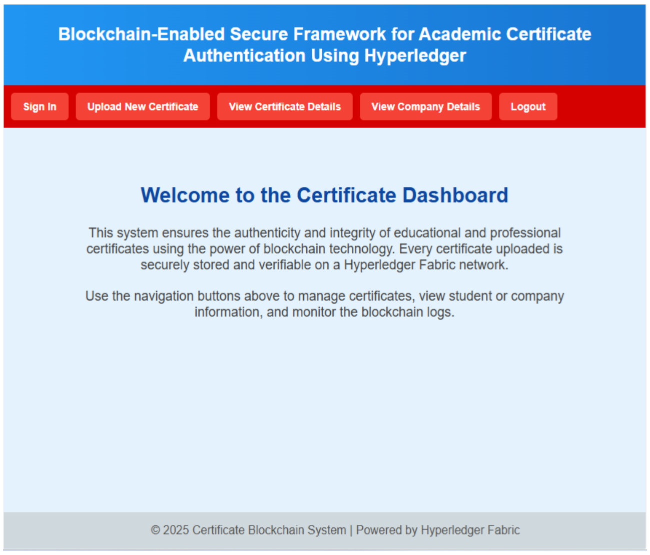
4. Smart Contract Execution (Issuance and Revocation): Smart contracts automate tasks like granting, updating, and revoking credentials. For example, if a certificate needs to be revoked due to error or fraud, the smart contract will label it as 'Revoked' on the blockchain. This modification is immediately visible to verifiers, ensuring transparency and trust without requiring manual action.

$$\mathrm{SC}(\mathrm{Action}, C_i) \rightarrow \text{Blockchain Update} \qquad (4)$$

$$\mathrm{SC}(\mathrm{Revoke}, C_i) \rightarrow \mathrm{Mark}(C_i, \mathrm{Status} = \mathrm{Revoked}) \qquad (5)$$

Algorithm 3: Correct Certificate (Admin Only)

```
CorrectCertificate(oldCertID, newCertID, updatedFields, newFileHash)
1. Get old certificate using oldCertID.
2. Return error if missing.
3. Create certificate object:
{ certificateID: newCertID, updatedFields, fileHash: newFileHash, status: "active", correctedFrom: oldCertID}
4. Mark old certificate as "superseded".
5. Record new certificate with newCertID.
6. Mark old ledger record "superseded".
7. Returned: "Certificate correction recorded successfully."
```



Blockchain-Enabled Secure Framework for Academic Certificate Authentication Using Hyperledger

Welcome to the Certificate Dashboard

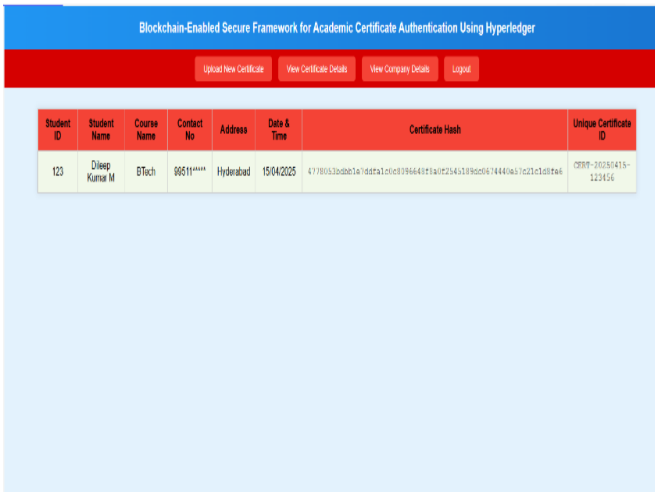
This system ensures the authenticity and integrity of educational and professional certificates using the power of blockchain technology. Every certificate uploaded is securely stored and verifiable on a Hyperledger Fabric network.

Use the navigation buttons above to manage certificates, view student or company information, and monitor the blockchain logs.

© 2025 Certificate Blockchain System | Powered by Hyperledger Fabric

Figure 2. Home page

The Figure 2 depicts a Blockchain-Enabled Secure Framework for Authenticating Academic Certificates with Hyperledger Fabric. This system provides a decentralised, tamper-proof environment in which educational and professional credentials can be safely submitted, saved, and verified. Stakeholders such as institutions, students, and companies can control certificate issuance, obtain certificate or company information, and confirm record validity via an easy-to-use interface. The integration with Hyperledger Fabric provides transparency, traceability, and data integrity, making credential verification more efficient, safe, and trustworthy.

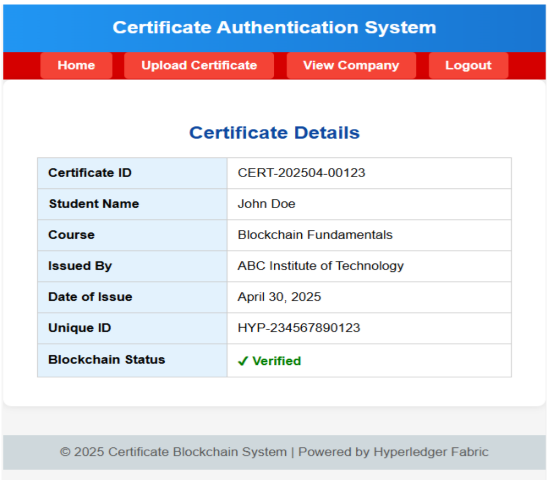

Blockchain-Enabled Secure Framework for Academic Certificate Authentication Using Hyperledger
Upload New Certificate
View Certificate Details
View Company Details
Logout

Student ID	Student Name	Course Name	Contact No	Address	Date & Time	Certificate Hash	Unique Certificate ID
123	Dileep Kumar M	BTech	99511*****	Hyderabad	15/04/2025	4778053bdbb1e7ddfa1c0c8096648f8a0f2545189dc0674440a57c21c1d8fe6	CERT-20250415-123456

Figure 3. Certificate's digital signature

Figure 3 shows how to use the certificate's digital signature to create a Unique ID. You can then attach it on paper. This Unique ID contains a digital signature and a physical link to Blockchain certificate data. Next, attach the Unique ID to the student's certificate.

Figure 4 shows how "View Certificate Details" lets users view and verify all the information on a blockchain-stored academic or professional certificate. This option retrieves the student's identity, degree, issuing institution, year of issuance, and issuer digital signature. Blockchain transaction parameters such block hash and timestamp verify the certificate's legitimacy and integrity. Employers, institutions, and other verifiers can trust the certificate because it has not been altered or fabricated. This functionality is essential for transparency and real-time credential validation.

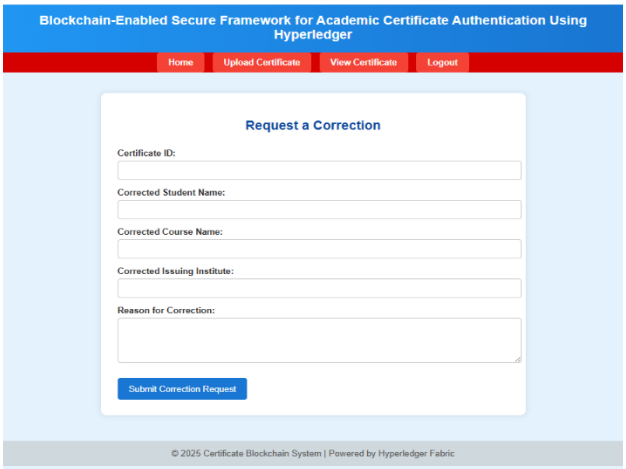


Certificate Details

Certificate ID	CERT-202504-00123
Student Name	John Doe
Course	Blockchain Fundamentals
Issued By	ABC Institute of Technology
Date of Issue	April 30, 2025
Unique ID	HYP-234567890123
Blockchain Status	✓ Verified

© 2025 Certificate Blockchain System | Powered by Hyperledger Fabric

Figure 4. Certificate details


Blockchain-Enabled Secure Framework for Academic Certificate Authentication Using Hyperledger
Home
Upload Certificate
View Certificate
Logout
Submit Correction Request

Request a Correction

Certificate ID:

Corrected Student Name:

Corrected Course Name:

Corrected Issuing Institute:

Reason for Correction:

© 2025 Certificate Blockchain System | Powered by Hyperledger Fabric

Figure 5. Correct certificate details

Figure 5 shows how the "Update/Correct Certificate Details" tool corrects name spelling, degree title, and graduation year or post-issuance modifications. Direct data modification is prohibited on Hyperledger Fabric blockchains for immutability. This function normally link the updated certificate to the original via the issuing authority's digital signature. Former certificates can be "revoked" or "superseded." This method guarantees data integrity, auditability, and transparent credential management.

5. ANALYSIS OF RESULTS

We used BAIUST data to compare the time to import data from Bitcoin-based blockchains and Ethereum frameworks to evaluate Hyperledger in our certification system. Table 1 data is used to compare three blockchain systems' computational lengths in Figure 6. Hyperledger was the best solution for our system after considering all options.

Table 1. Time required to complete transactions on multiple blockchain technologies

Number of Transactions	Hyperledger Duration (s)	Ethereum Duration (s)	Bitcoin Duration (s)
400	8.61	46.75	48.94
600	12.92	65.63	70.98
800	17.22	84.51	93.02
1000	21.53	103.39	115.06
1200	25.84	122.27	137.10
1400	30.15	141.15	159.14

Protecting the integrity of the Hyperledger Fabric is a top priority for the research. However, there is no short cut to determining a Hyperledger Fabric network's security; rather, it requires constant vigilance, analysis of policy implications, and investigation of technical details. It is critical to perform security audits on a regular basis and apply updates as needed in order to adequately handle the constantly changing threats and vulnerabilities. In order to keep the Hyperledger Fabric network secure, it is crucial to collaborate with security professionals and keep up with the newest innovations in blockchain security. Here we see the function of security measures as a constraint on technology. Fabric is a sturdy platform with a solid implementation, according to Linux's security evaluation. The platform features excellent security and functionality, allowing for future enhancements including correcting industry-standard cryptographic flaws. Measurement of a blockchain network's efficiency is as vital as security. Using Hyperledger calliper, we compared the created network's read-write throughput against Ethereum and Bitcoin.

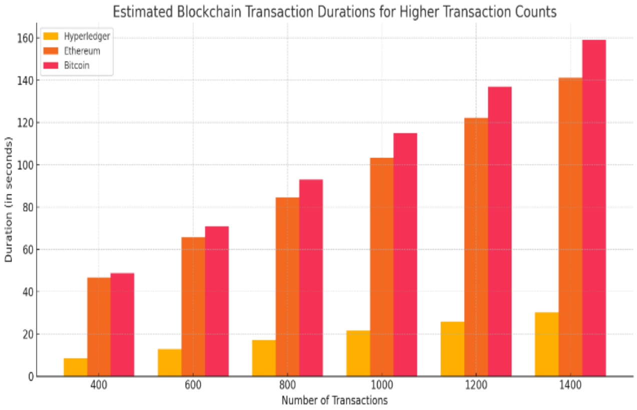


Figure 6. Compare three blockchain systems' computation time

Table 2. Different blockchain platforms' transaction throughput

Number of Transactions	HLF (TPS)	Bitcoin (TPS)	Ethereum (TPS)
400	280	12	26
600	220	14	22
800	130	13	28
1000	160	15	21
1200	165	13	20
1400	150	16	23

Table 2 compares Hyperledger Fabric (HLF), Bitcoin, and Ethereum Transactions Per Second (TPS) under 400–1400 transaction loads. Due to its efficient, permissioned consensus process, Hyperledger Fabric frequently beats others at 280 TPS. Due to their public, decentralised nature and consensus limits, Bitcoin and Ethereum have low and consistent TPS values of 13–16 and 20–28, respectively. This comparison shows Hyperledger Fabric's greater scalability and applicability for high-throughput enterprise applications like secure certificate authentication. Figure 7 depicts the Bitcoin and Ethereum transaction volumes compared to HLF.

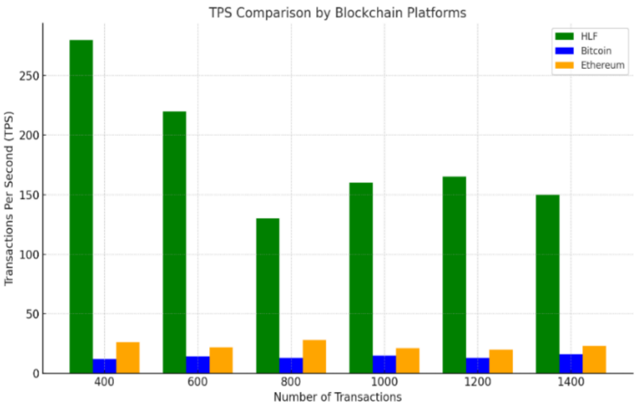


Figure 7. Bitcoin and Ethereum transaction volumes compared to HLF

The bar graph compares Hyperledger Fabric (HLF), Bitcoin, and Ethereum Transactions Per Second (TPS) at 400–1400 transaction volumes. Each cluster of bars indicates a transaction number, providing visual comparison between the three blockchain platforms. HLF (green) routinely outperforms Bitcoin (blue) and Ethereum (orange) in TPS values, demonstrating its better performance and scalability. In contrast, Bitcoin and Ethereum have low and steady TPS, indicating their inherent throughput restrictions under rising transaction loads.

Table 3. Read and write transaction performance in Hyperledger Fabric

Number of Transactions	Read TPS	Write TPS
400	220	80
600	210	145
800	90	165
1000	150	150
1200	145	125
1400	90	85

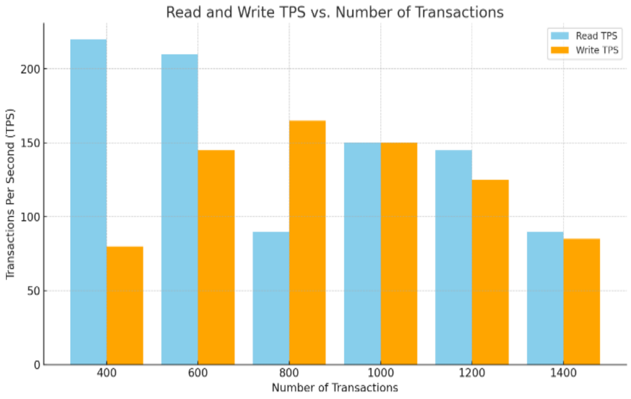


Figure 8. Reading and writing transaction speeds in milliseconds

Table 4. Transaction latency

Number of Participants	Latency Average (ms)	Average Delay per Person (ms)	Number of Participants
20	320	~25 (ms)	20
40	450	~25 (ms)	40
60	640	~25 (ms)	60
80	790	~25 (ms)	80
100	920	~25 (ms)	100

Table 3 shows the system's Read and Write TPS as transactions increase from 400 to 1400. Lower transaction loads initially yield good read efficiency (220 TPS at 400 transactions) and modest write performance. Read throughput falls with transaction count, but write throughput initially improves, peaking at 165 TPS for 800 transactions. After that, read and write TPS decline, suggesting resource saturation or network restrictions. In blockchain systems, read and write operations compete for system resources, influencing throughput and performance.

As transactions increase, Read and Write TPS vary as seen in Figure 8. The Read TPS starts high at 220 for 400 transactions but drops sharply at 800 transactions, suggesting read performance degradation under greater loads. At 1000 transactions, it recovers marginally but then drops. However, Write TPS progressively rises from 80 at 400 transactions to

165 at 800 transactions, indicating improved write processing with higher load. After 800 transactions, it declines and aligns with Read TPS later. As transaction volume increases, read and write operations compete for system performance.

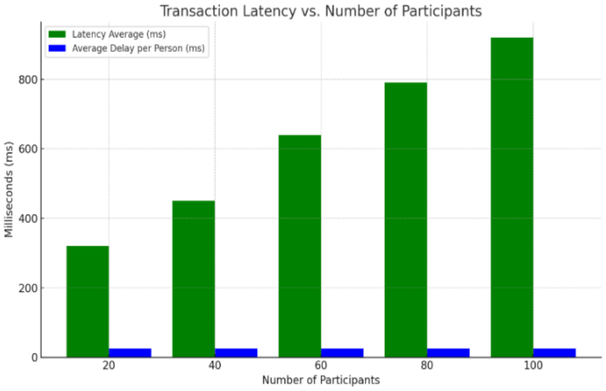


Figure 9. Assessment of network latency

The Table 4 shows that average transaction latency increases with participant count, indicating increased system load or more sophisticated coordination. While system latency increases with additional users, the average delay per person remains about 25 ms, demonstrating that the impact on individual users remains stable. This may suggest an efficient delay distribution across participants as the system scales.

The results of the network latency test (the time it takes for a transaction to be committed) are shown clearly in Figure 9. Both the mean delay and the mean delay per participant grow in proportion to the sample size. When looking at the results for 20, 40, 60, 80, and 100 participants, with average delay values of 306.5ms, 430ms, 603.7ms, 780.9, and 911.3ms, respectively, this association becomes clear. It should be mentioned that the typical lag time per user is around 12 to 14 milliseconds.

5.1 Comparative implications

Table 5 shows a comparison of three well-known blockchain platforms Hyperledger, Ethereum, and Bitcoin based on important technological factors that are important for managing digital certificates. The comparison looks at things like average transaction throughput (TPS), consensus processes, network design (public or permissioned), average latency, and how well they can be used to issue and verify certificates.

Table 5. Evaluation of blockchain platforms based on TPS, consensus, and certificate suitability

Platform	TPS (Avg)	Consensus Type	Architecture	Latency (Avg)	Public/Private	Suitability for Certificates
Hyperledger	250–280	PBFT / Raft	Permissioned	~300–900 ms	Private	High
Ethereum	20–28	PoW / PoS	Public	~5–10 sec	Public	Moderate
Bitcoin	13–16	PoW	Public	~10–60 min	Public	Low

•Bitcoin and Ethereum are not well-suited for educational certificate systems due to their long transaction confirmation times, energy inefficiency, and public visibility of data, which raises privacy concerns.

•Ethereum, with its support for smart contracts, is more flexible than Bitcoin but suffers from gas fees and scalability issues unless Layer 2 solutions are adopted.

•Hyperledger Fabric, by contrast, provides a modular, permissioned framework that supports fine-grained access control, identity management, and low-latency consensus, making it a strong candidate for institutional certificate verification platforms.

5.2 Practical implications

Scalability: The ability of Hyperledger Fabric to maintain a high throughput under varying transaction loads demonstrates its capacity to support large-scale deployments across multiple institutions.

Security: Fabric's permissioned model, combined with identity-based access control and audit trails, ensures data integrity and restricts unauthorised access critical for sensitive educational records.

Resource Allocation: The drop in performance at large loads shows how important it is to optimise network components (such ordering service and peer node scalability) and do load balancing to keep performance up.

Latency Tolerance: Even while latency goes up as the system gets bigger, it still responds quickly enough for most verification jobs. This means that users should have a satisfactory experience even when the network is under considerable stress.

6. DISCUSSION

The suggested certificate verification method based on Hyperledger Fabric has several advantages when it comes to performance, security, and use in large businesses. Its permissioned design, efficient consensus process, and support for smart contracts let institutions issue, check, and audit educational certificates in a way that is both open and safe. Moreover, the system supports immutable transaction logs, real-time access tracking, and granular role-based access control, all of which contribute to trust, reliability, and fraud prevention. However, several limitations must be acknowledged to provide a comprehensive assessment and guide future development:

6.1 Privacy protection

Although the platform employs a permissioned blockchain to restrict access, privacy remains a concern, particularly when sensitive personal data (e.g., student names, grades, or national IDs) is stored or linked. The immutable nature of blockchains means that once data is written, it cannot be removed, which conflicts with privacy regulations such as GDPR's right to be forgotten.To address this, future implementations should consider:

•Off-chain storage of personal or identifiable information using secure, encrypted databases, while only storing hashed references on-chain.

•Integration of zero-knowledge proofs (ZKPs) or confidential transactions to verify certificate data without revealing its content.

•Employing channel-based privacy and private data collections available in Hyperledger Fabric to ensure data isolation among authorised institutions.

6.2 Data scalability and network growth

As the number of participants, institutions, and issued certificates grows, so does the volume of data and network complexity. The current implementation has shown signs of resource saturation at higher transaction volumes (over 1000), which could impact system responsiveness and reliability at scale.To mitigate scalability issues:

•Sharding or partitioning of the ledger could be introduced to divide the network into manageable subsets.

•Leveraging sidechains or Layer 2 solutions may offload certain operations while maintaining the integrity of the main chain.

•Implementing automated resource scaling and performance tuning for peer nodes and orderers can ensure high availability and sustained throughput under variable loads.

6.3 Interoperability and standardisation

The system is designed to serve a consortium of educational institutions, but current blockchain deployments often suffer from interoperability challenges. Institutions may use different platforms or schemas, complicating cross-chain certificate verification. Future work should focus on:

•Adoption of interoperable standards like W3C's Verifiable Credentials and the Blockcerts open standard.

•Development of cross-chain bridges or APIs that allow institutions using other blockchain frameworks (e.g., Ethereum-based solutions) to interact securely with the Hyperledger-based network.

6.4 Usability and adoption barriers

The integration of blockchain technology in academic ecosystems also depends on its usability and cost-effectiveness. While the system is technically sound, user training, administrative overhead, and system onboarding need further exploration. Potential improvements include:

•Simplifying certificate issuance and verification interfaces using user-friendly dashboards and mobile apps.

•Designing smart contract templates for academic institutions to reduce the technical barrier to adoption.

Offering self-sovereign identity (SSI) support, enabling students to manage and share credentials independently.

7. CONCLUSIONS

We created a secure academic credential management system based on Hyperledger Fabric for this project. Its goal was to deal with the growing problems of certificate fraud, data tampering, and slow verification processes. Hyperledger Fabric's permissioned design makes it easy to issue, store, and validate academic credentials in a way that is safe from tampering and protects privacy. Institutions can give out degrees and transcripts that are permanently stored on the blockchain. Students and employers can then verify these documents in real time without having to go through middlemen. The system's role-based access control makes sure that only users who are allowed to can access certain data. This makes the system more secure and protects the data. The proposed Hyperledger-based platform is better for academic use than public blockchains like Ethereum or Bitcoin because it offers better privacy, institutional governance, and scalability. Public blockchains disclose transactional metadata and require bitcoin to work. Even while it has some good points, the suggested system has a lot of problems. There are also privacy issues, especially when sensitive user info is stored directly on-chain. To follow privacy laws like GDPR, this data needs to be stored off-chain or with advanced cryptographic methods. Scalability is another problem; the system starts to run out of resources when there are a lot of transactions, which slows down read and write throughput. The platform also doesn't support cross-chain interoperability for now, which makes it harder for it to operate with other blockchain frameworks or organisations that use other infrastructures. From a usability point of view, technical intricacy may make it hard for non-expert users, such students and administrative staff, to use.

Several improvements are suggested to get around these problems. Off-chain storage that is linked to on-chain hashes can help protect privacy while keeping data safe. Using zero-knowledge proofs and private data collectors might help protect sensitive information even further during verification. Using global standards like W3C Verifiable Credentials and Blockcerts would make it easier for different systems to work together. Also, making interfaces and mobile apps that are easy to use can make things a lot easier to access and use. Using solutions that boost performance, like as sharding and sidechains, can help increase throughput and make room for future development. Cross-chain bridges and smart contracts that work with other platforms should be the main focus of future development. The system should also be tested in large-scale, multi-institutional situations to see how well it can adapt and how strong it is. Integrating self-sovereign identification (SSI) models would provide users more control over their credentials, which is in line with new developments in digital identity management. Adding AI-driven technologies could also help with fraud detection and system monitoring. Long-term security audits and checks to make sure that rules are being followed will be important for keeping trust and staying safe from new cyber threats. By working on these things, the system can become a scalable, safe, and trusted solution for checking academic credentials all around the world.

REFERENCES

[1] Tariq, A., Haq, H.B., Ali, S.T. (2022). Cerberus: A blockchain-based accreditation and degree verification system. IEEE Transactions on Computational Social Systems, 10(4): 1503-1514. https://doi.org/10.1109/TCSS.2022.3188453

[2] Roopa, C., Suganthe, R.C., Shanthi, N. (2020). Blockchain based certificate verification using ethereum and smart contract. Journal of Critical Reviews, 7(9): 330-336.

[3] Murala, D.K. (2024). Corrections to “Metaeducation: State-of-the-art methodology for empowering feature education”. IEEE Access, 12: 166459-166459. https://doi.org/10.1109/ACCESS.2024.3487030

[4] Dalal, J., Chaturvedi, M., Gandre, H., Thombare, S. (2020). Verification of identity and educational certificates of students using biometric and blockchain. In Proceedings of the 3rd International Conference on

Advances in Science & Technology (ICAST).

[5] Leka, E., Selimi, B. (2021). Development and evaluation of blockchain based secure application for verification and validation of academic certificates. Annals of Emerging Technologies in Computing (AETiC), 5(2): 22-36. https://doi.org/10.33166/AETiC.2021.02.003

[6] Leka, E., Kordha, E., Hamzallari, K. (2022). Towards an IPFS-blockchain based authentication/management system of academic certification in western Balkans. In 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, pp. 1448-1453. https://doi.org/10.23919/MIPRO55190.2022.9803625

[7] Effiong, M., Norta, A., Udokwu, C., Hattingh, M. (2022). Adoption of blockchain technology in academic certificate-verification systems. In 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), Irvine, CA, USA, pp. 1-6. https://doi.org/10.1109/iGETblockchain56591.2022.10087108

[8] Kumar, K.D., Senthil, P., Kumar, D.M. (2020). Educational certificate verification system using blockchain. International Journal of Scientific & Technology Research, 9(3): 82-85.

[9] Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R., Raghavendran, C.V., Lalitha, R.V.S., Annapurna, B. (2021). Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP Journal on Information Security, 2021(1): 1-9. https://doi.org/10.1186/s13635-021-00122-5

[10] Saleh, O.S., Ghazali, O., Rana, M.E. (2020). Blockchain based framework for educational certificates verification. In Studies, Planning and Follow-up Directorate. Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia.

[11] Rahman, M.M., Tonmoy, M.T.K., Shihab, S.R., Farhana, R. (2023). Blockchain-based certificate authentication system with enabling correction. Journal of Computer and Communications, 11(3): 73-82. https://doi.org/10.4236/jcc.2023.113006

[12] Murala, D.K., Loucif, S., Rao, K.V.P., Hamam, H. (2025). Enhancing smart contract security using a code representation and GAN based methodology. Scientific Reports, 15(1): 15532. https://doi.org/10.1038/s41598-025-99267-3

[13] Nguyen, M.D., Nguyen-Dinh, C.H., Phuong, L.A. (2022). Boca: A novel semantic blockchain-based authentication system of educational certificates. International Journal of Computers and Applications, 44(11): 1074-1082. https://doi.org/10.1080/1206212X.2022.2111509

[14] Murala, D.K., Panda, S.K., Sahoo, S.K. (2023). Securing electronic health record system in cloud environment using blockchain technology. In Recent Advances in Blockchain Technology: Real-World Applications, Springer International Publishing, pp. 89-116. https://doi.org/10.1007/978-3-031-22835-3_4

[15] Lutfiani, N., Apriani, D., Nabila, E.A., Juniar, H.L. (2022). Academic certificate fraud detection system framework using blockchain technology. Blockchain Frontier Technology, 1(2): 55-64. https://doi.org/10.34306/bfront.v1i2.55

[16] Mondal, S., Panja, A., Karforma, S. (2023). An efficient e-certificate management system in e-learning using blockchain. Science and Culture, 89(3-4): 120-124.

[17] Nousias, N., Tsakalidis, G., Michoulis, G., Petridou, S., Vergidis, K. (2022). A process-aware approach for blockchain-based verification of academic qualifications. Simulation Modelling Practice and Theory, 121: 102642. https://doi.org/10.1016/j.simpat.2022.102642

[18] Murala, D.K. (2024). Blockchain-based internet of efficient healthcare data sharing and monitoring things. In International Conference on Frontiers of Intelligent Computing: Theory and Applications, Singapore, pp. 269-279. https://doi.org/10.1007/978-981-96-0139-4_22

[19] Badhe, V., Nhavale, P., Todkar, S., Shinde, P., Kolhar, K. (2020). Digital certificate system for verification of educational certificates using blockchain. International Journal of Scientific Research in Science and Technology, 7(5): 45-50.

[20] Maestre, R.J., Bermejo Higuera, J., Gámez Gómez, N., Bermejo Higuera, J.R., Sicilia Montalvo, J.A., Orcos Palma, L. (2023). The application of blockchain algorithms to the management of education certificates. Evolutionary Intelligence, 16(6): 1967-1984. https://doi.org/10.1007/s12065-022-00812-0

[21] Lamkoti, R.S., Maji, D., Gondhalekar, A.B., Shetty, H. (2021). Certificate verification using blockchain and generation of transcript. International Journal of Engineering Research & Technology, 10(3): 539-544.

[22] Sultana, S.A., Rupa, C., Malleswari, R.P., Gadekallu, T.R. (2023). IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field. Information, 14(8): 446. https://doi.org/10.3390/info14080446

[23] Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D., Jing, J. (2020). Blockchain-based certificate transparency and revocation transparency. IEEE Transactions on Dependable and Secure Computing, 19(1): 681-697. https://doi.org/10.1109/TDSC.2020.2983022

[24] Murala, D.K. (2024). METAEDUCATION: State-of-the-art methodology for empowering feature education. IEEE Access, 12: 57992-58020. https://doi.org/10.1109/ACCESS.2024.3391903

[25] Singh, J., Rani, S., Kumar, V. (2024). Role-based access control (RBAC) enabled secure and efficient data processing framework for IoT networks. International Journal of Communication Networks and Information Security, 16(2): 91-103.

[26] Li, S., Wang, J., Ji, W., Chen, Z., Song, B. (2024). A hybrid storage blockchain-based query efficiency enhancement method for business environment evaluation. Knowledge and Information Systems, 66(10): 6307-6335. https://doi.org/10.1007/s10115-024-02144-0

[27] Xu, X. (2024). Zero-knowledge proofs in education: A pathway to disability inclusion and equitable learning opportunities. Smart Learning Environments, 11(1): 7. https://doi.org/10.1186/s40561-024-00294-w

[28] Panda, S.K., Satapathy, S.C. (2021). An investigation into smart contract deployment on Ethereum platform using Web3.js and solidity using blockchain. In Data Engineering and Intelligent Computing: Proceedings of ICICC 2020, Singapore, pp. 549-561. https://doi.org/10.1007/978-981-16-0171-2_52

[29] Panda, S.K., Rao, D.C., Satapathy, S.C. (2021). An

investigation into the usability of blockchain technology in Internet of Things. In Data Engineering and Intelligent Computing: Proceedings of ICICC 2020, Singapore, pp. 563-572. https://doi.org/10.1007/978-981-16-0171-2_53

[30] Panda, S.K., Dash, S.P., Jena, A.K. (2021). Optimization of block query response using evolutionary algorithm. In Data Engineering and Intelligent Computing: Proceedings of ICICC 2020, Singapore, pp. 573-579. https://doi.org/10.1007/978-981-16-0171-2_54

[31] Nanda, S.K., Panda, S.K., Das, M., Satapathy, S.C. (2022). Automating vehicle insurance process using smart contract and Ethereum. In Advances in Micro-Electronics, Embedded Systems and IoT: Proceedings of Sixth International Conference on Microelectronics, Electromagnetics and Telecommunications (ICMEET 2021), Singapore, pp. 237-247. https://doi.org/10.1007/978-981-16-8550-7_23

[32] Varaprasada Rao, K., Panda, S.K. (2022). Secure electronic voting (E-voting) system based on blockchain on various platforms. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Singapore, pp. 143-151. https://doi.org/10.1007/978-981-19-1976-3_18

[33] Varaprasada Rao, K., Panda, S.K. (2022). A design model of copyright protection system based on distributed ledger technology. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Singapore, pp. 127-141. https://doi.org/10.1007/978-981-19-1976-3_17