Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

EduVeriChain: A Blockchain-Based System for Secure Academic Credential Verification and Management

Sheela D V *

*Corresponding author, Research Scholar, School of Science & Computer Studies, CMR University, Bengaluru, Karnataka, India. E-mail: sheela.dv@cmr.edu.in

Ashok Kumar T A

Professor and Director, School of Science & Computer Studies, CMR University, Bengaluru, Karnataka, India. E-mail: ashokkumar.t@cmr.edu.in

Journal of Information Technology Management, 2025, Vol. 18, Issue 1, pp. 158-183
Published by the University of Tehran, College of Management
doi: https://doi.org/10.22059/jitm.2026.106536
Article Type: Research Paper

Received: August 26, 2025
Received in revised form: September 27, 2025
Accepted: December 19, 2025
Published online: January 20, 2026

Abstract

Academic credential fraud is a pervasive issue with significant implications for educational institutions, employers, and society as a whole. The centralized nature of traditional academic verification systems makes them vulnerable to inefficiencies, corruption, and forgery, highlighting the need for a more secure and transparent solution. Blockchain technology provides a decentralized, tamper-proof framework for managing digital credentials, ensuring authenticity and integrity without intermediaries. This research proposes EduVeriChain, a blockchain-based system for securely issuing, verifying, and managing academic credentials. Utilizing smart contracts, decentralized storage via the InterPlanetary File System (IPFS), and robust encryption, EduVeriChain ensures the transparency, security, and immutability of academic records. The system's Credential Revocation Authority (CRA) and Credential Status Enforcer (CSE) provide automated and secure revocation, further enhancing trust. Performance evaluation reveals that EduVeriChain achieves high throughput, low latency, and predictable costs, making it a scalable and practical solution for academic credential verification. By providing a decentralized, secure, and efficient framework, EduVeriChain aims to mitigate pervasive document fraud and promote integrity in academic credential management.

Keywords: Academic Credential Verification, EduVeriChain, Smart Contracts, InterPlanetary File System (IPFS), Credential Fraud Prevention, Decentralized Storage

Introduction

Higher educational institutions and universities play a pivotal role in fostering social mobility, driving economic progress, and developing a skilled workforce that contributes to global well-being. As digital transformation reshapes how individuals engage with education, the demand for accessible, flexible, and high-quality learning has increased significantly (Diaz-Infante et al., 2022). From bachelor's to doctoral students, as well as lifelong learners, more individuals are using online tools to learn and improve their skills. This evolution not only enhances individual growth but also fosters innovation in the job market to meet both local and international employment requirements. Academic certificates and degrees issued by recognized institutions serve as official documentation of an individual's educational achievements (Alam et al., 2021; Bajwa et al., 2018).

These documents are essential for employers, recruitment agencies, and other organizations, such as universities, multinational corporations, and government entities, to assess whether a candidate possesses the necessary knowledge and technical skills for specific job roles (Hope et al., 2018). However, the integrity of these academic credentials is under growing threat due to increasing incidents of fraud, dishonesty, and bribery in the education sector. Numerous studies and reports have highlighted the prevalence of document forgery and malpractice in credential verification and attestation processes (Bautista et al., 2016). This issue is particularly severe in developing countries like India, where systemic weaknesses in academic governance have led to widespread cases of misrepresentation and forgery of academic documents (Rustemi et al., 2023). Such cases of fake and forged academic credentials are being identified, successfully investigated, and reported (Kwok et al., 2022; Bhaskar et al., 2021). Reports indicate that over one-third of job applicants have admitted to using fake degrees to secure employment (Kim et al., 2022; Fartitchou et al., 2025). Additionally, research shows that approximately 5,000 unrecognized universities and institutes worldwide issue over 200,000 fake or forged degrees annually, generating earnings exceeding $1 billion (Hope et al., 2018). According to a recent Forbes study, the degree mill industry is estimated to generate $7 billion a year worldwide in fraudulent diplomas and transcripts (Bautista et al., 2016).

Consequently, to avoid further negative impact on society, this problem must be prevented. Traditionally, the certification authority verifies diplomas or certificates, as it is difficult to distinguish genuine from fake certificates without specialized tools and knowledge that the certificate issuer alone can provide. In recent years, blockchain has emerged as a promising technology that automatically records and verifies transactions (Rustemi et al., 2023). Blockchain is a cryptographically secure protocol that maintains an immutable digital ledger of asset transactions across a public or private peer-to-peer network. Its key features, including decentralization, transparency, trust, and elimination of a single point of failure, make it a strong candidate for use in academic credential verification. Although widely

adopted in finance and business, blockchain's application in the education sector has recently gained traction (Schmidt et al., 2016). Nevertheless, blockchain-based systems still face several challenges. Issues such as performance limitations, data immutability, scalability, and reliance on consensus algorithms hinder practical implementation. Many existing systems depend on human involvement and lack support for dynamic updates or retroactive verification of previously issued degrees (Fartitchou et al., 2025).

The Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, has introduced Blockcerts as an open standard for academic credentials on the blockchain, which can be freely used to authenticate academic credentials. However, we have identified three limitations of Blockcerts: 1) Blockcerts changes the existing workflow of degree issuance and is difficult for degree-awarding institutes to adopt; 2) it only operates over degrees or certificates individually issued in digital form; and 3) it does not offer any solution for degrees that have already been issued to previously graduated students (Savelyeva et al., 2022). Despite these technological advancements, the use of blockchain smart contracts for preventing degree certificate forgery remains limited and speculative. Forgery of academic documents, including diplomas and transcripts, continues to pose a significant challenge, underscoring the need for more robust, scalable, and institution-friendly solutions to secure the integrity of educational credentials.

Motivation and contributions

Academic credential fraud is a growing issue, with traditional centralized systems being costly and prone to forgery. Blockchain's decentralized, transparent architecture can eliminate intermediaries, reduce fraud, and ensure the secure management of academic records, despite efforts such as blockcerts. Integration challenges persist, underscoring the need for a scalable, compatible solution for existing systems. Additionally, blockchain offers a trusted way to manage digital credentials, advancing the credibility of online education and supporting lifelong learning. This research aims to develop EduVeriChain, a secure, efficient, and widely adoptable system for academic document verification.

Development of EduVeriChain for Academic Credential Verification: We propose EduVeriChain, a blockchain-based solution that leverages smart contracts and InterPlanetary File System (IPFS) to create a secure, transparent, and efficient system for issuing, storing, and verifying academic credentials. This approach ensures authenticity, prevents forgery, and eliminates the need for third-party verification.

Secure and Automated Credential Lifecycle Management: EduVeriChain introduces a robust framework for managing the entire credential lifecycle, including issuance, verification, access, and revocation. The use of smart contracts—such as Credential Revocation Authority (CRA) and Credential Status Enforcer (CSE)—ensures that all

operations are conducted securely and with multi-party approval, significantly reducing the risks of unauthorized access or revocation.

Efficient Encryption and Storage Mechanism: The research presents EduVeriChain Secure Encryption (ESE), a lightweight encryption technique for protecting academic records before storage in IPFS. This approach ensures that sensitive data remains secure while leveraging blockchain for immutability and transparency.

Enhanced Revocation Mechanism: EduVeriChain incorporates an innovative Credential Revocation Authority (CRA) and a Credential Status Enforcer (CSE) to automate and secure credential revocation. The multi-signature mechanism ensures that credentials are revoked only by authorized entities, which enhances the integrity of the verification system.

Performance Evaluation and Cost Analysis: We provide a detailed performance evaluation of the EduVeriChain system, analyzing its scalability, encryption time, storage efficiency, and associated costs (e.g., gas fees). The results indicate that the proposed solution maintains low latency and high throughput, making it efficient and cost-effective for practical use in academic institutions

Literature Review

Several certificate platforms and systems based in British Columbia, including those at the Open University, MIT, and the University of Nicosia, have been recently proposed and developed (Fartitchou et al., 2025; Durant et al., 2017; Schmidt et al., 2016; Fartitchou et al., 2025). To mitigate the issues of fraud, forgery, and inefficiencies encountered by both traditional and digital certificate systems, the platforms and systems leverage the security and transparency provided by blockchain technology. This section analyzes the advantages and disadvantages of digital certificate systems in the context of education in British Columbia, supported by pertinent research. To enhance the effectiveness and security of managing educational credentials, Han et al. (2018) proposed an innovative blockchain-based approach for verifying educational data. The system's decentralized architecture removes intermediaries, reduces verification costs, and empowers individuals to control their educational data while facilitating seamless communication among authorized institutions. The proposed method employs distinct private keys to ensure secure access to data and a consensus mechanism to validate transaction authenticity. To automate the issuance of degree certificates in Brazil and ensure the secure management of academic data, Palma et al (2019) proposed a blockchain-based system utilizing Solidity and Ethereum.

The system employs three SCs: authority, curriculum, and diploma, to mitigate fraud and enhance productivity. This guarantees that certificates can be issued and authenticated exclusively by authorized entities. The study illustrates BC's capacity to address privacy

concerns and costs, improve the security and transparency of academic credential management, and establish a basis for global adoption. Xie et al. (2020) proposed a decentralized approach to managing educational credentials using smart contracts on the Ethereum blockchain. This system employs smart contracts to securely manage certificate issuance, verification, and revocation, ensuring decentralization, transparency, and tamper-resistance. Several specialized contracts are employed, with each responsible for a specific phase of the certificate lifecycle. The integration of SC logic with cryptographic techniques enhances security by eliminating reliance on external systems and preventing unauthorized access. The system's architecture facilitates integration with existing protocols and provides greater flexibility for a broader range of applications. Saleh et al. (2020) proposed a blockchain-based system for verifying educational qualifications.

This framework addresses critical security vulnerabilities in existing systems by focusing on key components, including ownership, confidentiality, permissions, and authentication. An in-depth analysis of existing certification systems revealed that many systems inadequately address these critical components, creating vulnerabilities that could be exploited for fraudulent activities. The proposed method aims to enhance the verification process by leveraging Hyperledger Fabric. To enhance the security and traceability of degree attestation and verification processes in higher education, Ayub Khan et al. (2021) introduced an architecture known as the HEDU-ledger. This architecture uses Hyperledger Fabric to establish a private, permissioned blockchain network. This architecture provides a decentralized, immutable ledger for preserving academic credentials, effectively addressing critical issues such as data tampering, falsification, and the inefficiencies of traditional centralized systems. Kim et al. (2022) have developed an implementation model for a blockchain-based academic degree certification system via the start-up BeCertify. This method aims to resolve challenges related to accessibility and data management within the higher education sector. The proposal outlines a secure, transparent, and decentralized methodology for the issuance and validation of academic credentials.

Maestre et al. (2023) outline a verification procedure designed to reduce third-party access while ensuring the security and integrity of sensitive data. The implementation of blockchain technology for document verification is proposed as a solution to this issue—the system's enhanced decentralization reduces external entities' access to sensitive information. Blockchain technology enhances security by rendering documents immutable, thereby reducing the incidence of fraudulent activities such as identity theft and the establishment of fictitious accounts.

The three blockcert constraints previously identified have been resolved through the implementation of DocsChain (Mahlaba et al., 2022). Docschain seamlessly integrates with the existing degree-issuance system by using authentic copies of degree documentation. To facilitate understanding of the semantics associated with data captured at different locations

within the document, the record for each degree document is maintained in an up-to-date state, including details of the corresponding OCR template. The procedure used to execute this task is known as optical character recognition (OCR) (Rasool et al., 2020).

The implementation of blockchain technology for document verification is proposed as a solution to this issue. Consequently, the difficulty for external entities to access private information may increase, thereby reducing the system's overall centralization. Blockchain technology enhances security by ensuring that documents are immutable, thereby reducing the risk of fraudulent activities such as identity theft and the establishment of fictitious accounts (Mahlaba et al., 2022).

In their work, Fartitchou et al. (2025) introduced a blockchain-based certification system for academic degrees through the start-up BeCertify, aiming to improve the transparency, security, and accessibility of educational records. The paper discusses the different stages of platform development, including system architecture design and REST API functionality, and addresses the challenges encountered during implementation. The study emphasizes the significance of multi-signature authorization and the decentralized characteristics of blockchain, which provide both students and educational institutions greater control over the management of academic records.

Methodology

The proposed study uses blockchain technology, which securely and openly stores records. It is a decentralized database managed by a distributed network of computers. In this study, there are mainly four phases: Credential Holders (including the Credential Authority), Encrypting, Decrypting, and Blockchain. In this application situation, the sole responsibility for maintaining the application and overseeing its operations is taken over by the Credential Authority. A unique Identification is used by the Credential Authority to upload files. The information is encrypted and later stored in an InterPlanetary file system with the ID. The Credential Holders could later use this information. To ensure the information is not tampered with, a hash of the information is stored in the blockchain. Therefore, a record of the information, as well as its possession, is used to verify its authenticity. The Credential Authority uses the MetaMask Tool for interaction with the blockchain and for managing transaction information. The Credential Holder then decrypts this information. This model ensures that the Credential Holders view information that the Credential Authority securely stores, and that it remains secure and cannot be tampered with.

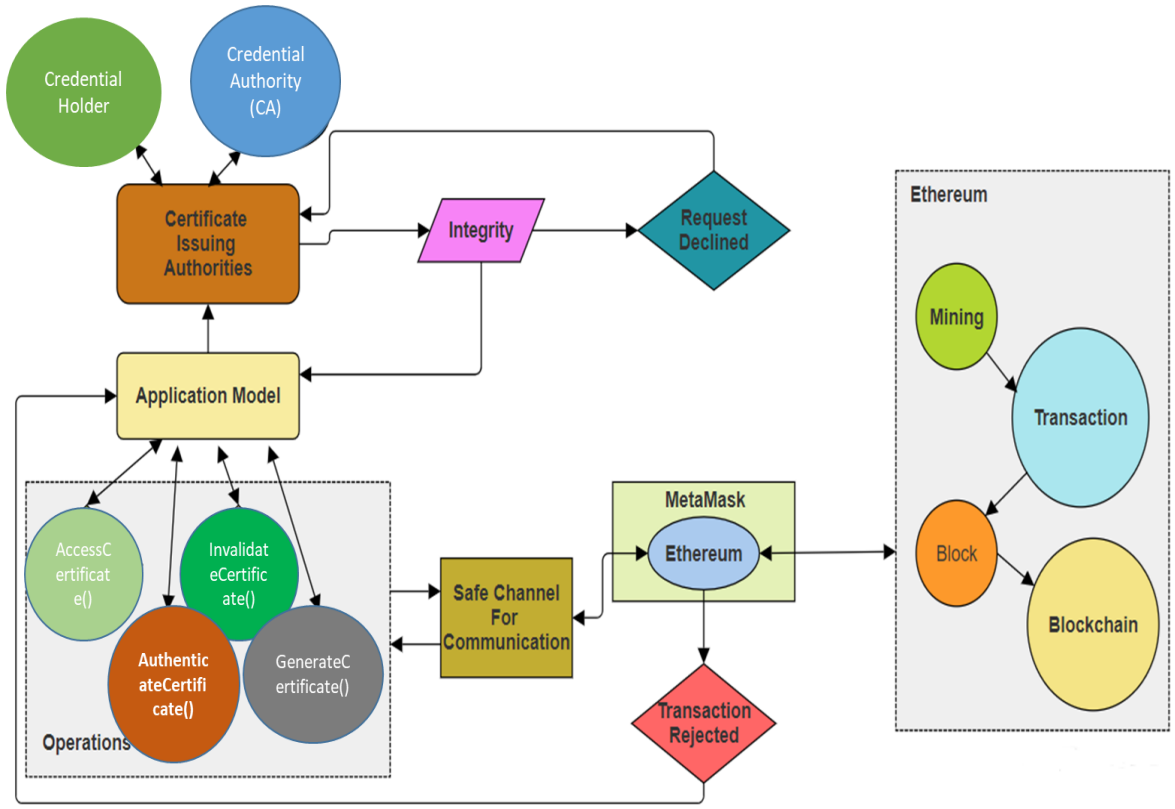

Figure 1. EduVeriChain model

Figure 1 below shows the workflow of the EduVeriChain model. We consider that the Generating Certificate Authorities must authenticate the request sent by the Credential Holder and the Credential Authority. If this verification fails, the request is disposed. However, if not, it is transferred to the application, where operations (including verification, Access Certificate, Invalidate Certificate, etc.) occur. Further, the input information undergoes EduVeriChain Secure Encryption (ESE) within the secure communication channel, and the output is passed to the Ethereum blockchain via MetaMask if the Ethereum balance exceeds the threshold score. In conclusion, the information is stored in blockchain. When the Ethereum balance falls below the threshold, the transaction is discarded and displayed to the application. To obtain information from the blockchain, EduVeriChain Secure Decryption (ESD) occurs in a secure channel and is then displayed to the application.

Credential Authority and Credential Holder

In phase 1, the main aspects include the Admin and the Credential Holder. The Credential Holder can retrieve and read the information after it is decrypted. In contrast, the Admin is responsible for uploading and securely storing it, managing the decentralized application, verifying the Credential Holder's authorization, and uploading and managing information to the model. Access to EduVeriChain Secure Encryption (ESE) for files before upload is granted to the Credential Authority. Permissions are set by the Credential Authority, which

manages access for the Credential Holder and ensures the EduVeriChain model operates smoothly without fault. The integrity and security of the information are solely the responsibility of the Credential Authority. The Credential Holder interaction includes actions or features that must be accessed. The Credential Holders possess the necessary access permissions to view and access the encrypted information files stored in the InterPlanetary file system.

EduVeriChain Secure Encryption (ESE)

In the second phase of EduVeriChain Secure Encryption (ESE), to ensure the information is secure and private, sensitive data exchanged between Credential Holders and the Credential Authority could be encrypted before being uploaded. The EduVeriChain algorithm used for EduVeriChain Secure Encryption (ESE) is both functional and lightweight. It is used for EduVeriChain Secure Encryption (ESE), which uses two keys. The information is converted to an unreadable format, making it difficult for unauthorized Credential Holders to understand or access. Algorithm 1 below shows the process of EduVeriChain Secure Encryption (ESE), which comprises two major stages: a Combinatorial Factor and operations related to the algorithm's functional-encryption nature, represented by FE_param_1 *and* FE_param_2. Here, FE_param_1 and FE_param_2 describe the functional encryption operations for division and modulus, respectively. There are two keys, the four dimensional based $(V_u \rightarrow \{V_{u0}, V_{u1}, \dots, V_{u(p-1)}\})$ and five dimensional based $\left(R_u \rightarrow \left\{R_{u0}, R_{u1}, \dots, R_{u(p-1)}\right\}\right)$, both having changing lengths which are random. Further, every element of plain text is transformed into the corresponding ASCII number $E_{cl} \leftarrow ACSII(E_l)$ as described in Figure 2 given below. Furthermore, the XOR operation is applied to $BinoCoeff_l \leftarrow E_{cl} \oplus V_{ul}$. Further, the division and modulus operations are applied to the given information using the five-dimensional key. The resulting information about division and modulus is combined into the characters 'h' and 't', leading to $EV_v \leftarrow concatentate(h,\ FJ_l, t,\ PJ_l)$.

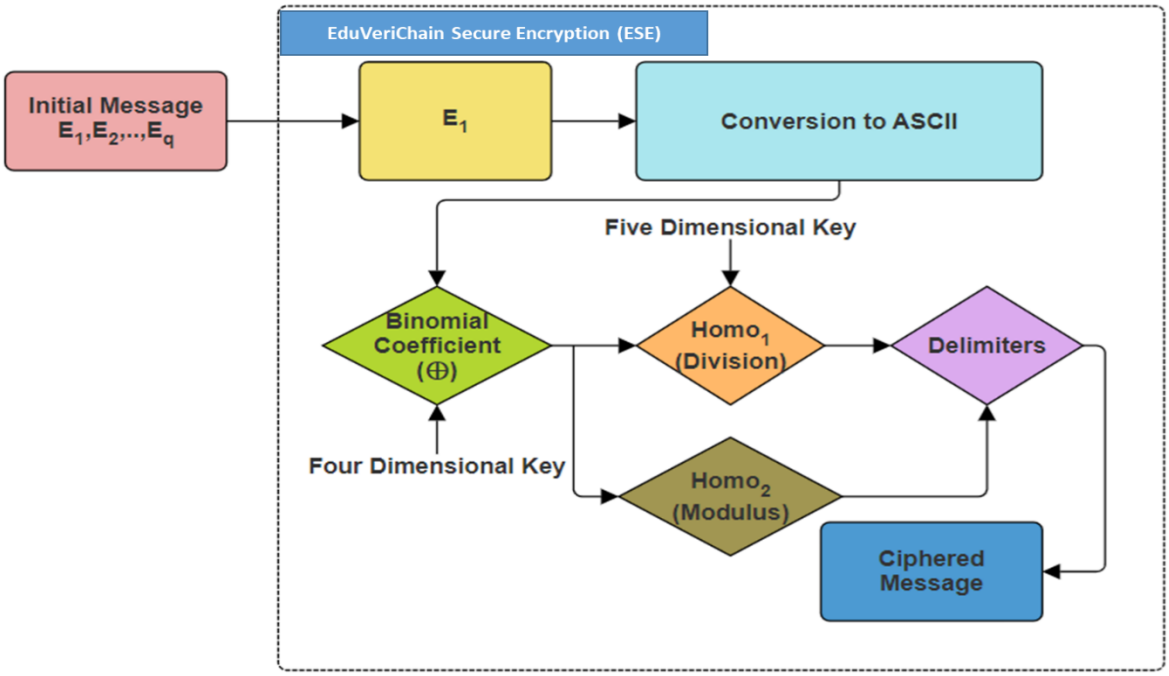

Figure 2. EduVeriChain Secure Encryption (ESE)

Also, there are two sets of operations performed by the Credential Authority and the Credential Holders. The Credential Authority is responsible for operations, including Registration, in which every Credential Authority must register with a unique ID. GenerateCertificate() where the Credential Holder file IDs, the nature of the certificate, its issuer, the Credential Holder, and the date are essential information. Details of the Certificate are implemented using the Credential Holder's ID and data from the blockchain, similar to the Credential Holder's certificate. AuthenticateCertificate () requires the ID and the registration number for certificate verification. Authentication (), is it essential for the Credential Authority to be authorized to have access to the details of the certificate. The operations performed by the Credential Holder include Registration, during which every Credential Holder must have a unique ID. In AuthenticateCertificate (), the ID and the registration number are required to verify the certificate. Authentication (), the details of the certificate cannot be accessed by the Credential Holder unless they are authorized.

Algorithm 1 **EduVeriChain Secure Encryption (ESE) Algorithm**

Input Initial Data

Output Ciphered Data

Step1 The initial text data is read as

$$E \leftarrow (E_0, E_1, E_2, \dots, E_{(p-1)})$$

Step2 Production of keys is done at random,

Four-dimensional Secret key $V_u \rightarrow \left(V_{u0}, V_{u1}, \ldots, V_{u(p-1)}\right)$

Five-dimensional Secret key $R_u \rightarrow (R_{u0}, R_{u1}, \ldots, R_{u(p-1)}$

Step 3 For $l = 0$ to $p - 1$ do till step 7

Step 4 Transform to an ASCII score for every character

$E_{cl} \leftarrow ACSII(E_l)$

Step 5 The ACSII of the initial data is used to obtain the Combinatorial Factor

$BinoCoeff_l \leftarrow E_{cl} \oplus V_{ul}$

Step 6 The operations FE_param_1, FE_param_2 are applied on $BinoCoeff_l$

$FJ_l \leftarrow division(BinoCoeff_l,\ R_{ul})FE\_param_1$:

$PJ_l \leftarrow modulus(BinoCoeff_l,\ R_{ul})FE\_param_2$:

Step 7 The result of step 6 is concatenated

$EV_v \leftarrow concatentate(h,\ FJ_l, t,\ PJ_l)$

Step 8 Result Ciphered Data EV_v

Eduverichain Blockchain Mechanism

This mechanism is a ledger technology that is decentralized and distributed, making it possible to record transactions and store information in a secure way. It is a chain of blocks that are interlinked, each containing a set of transactions or information and linked to the previous block using a hash function. This link results in a permanent transaction record and information on the blockchain. The main characteristic of blockchain is its decentralization. This network involves multiple computers in the authentication process. The network's security is enhanced because no single point of failure occurs due to the blockchain's decentralized nature. The cryptocurrencies often used in blockchain technology are Ethereum and Bitcoin.

The antifalsification solution for academic diplomas and certificates, built on the Ethereum blockchain, is deployed through a web application. The InterPlanetary File System

assigns every file a unique identifier, making it easier to identify and verify. These IDs are stored on the blockchain to enhance security against intruders. When the Credential Authority or the Credential Holder have the need to access information from InterPlanetary file system, is it essential for verification of the ID. After ID confirmation, a hash score is retrieved from the blockchain. MetaMask is used to access Ethereum. Ethereum is a monetary unit required for transactions on the blockchain network. Algorithm 2, given below, is used to identify the Credential Holder and the Credential Authority, as well as to block development. In this case, the Credential Holder is asked to enter the required credentials: $Application_{Info} \leftarrow Name(, Credential\ Authority\ (CA), Credential\ Holder\ (CH)) \| , Password(, Credential\ Authority\ (CA), and\ User) \| Authority_{Name}$. Furthermore, once integrity verification is complete, $Application_{info}$ completes the credentials produced by the Credential Holder or the Credential Authority. Only if the provided details are valid is an ID issued. Otherwise, the request is declined. The Encrypted certificate authorities' information $G(CF)$ is stored in the InterPlanetary file system once the Credential Authority is authenticated, and the related ID of the encrypted information, DEV_{id} hash score $G(EV)$, is stored in the blockchain. Before storage, the Ethereum balance must be verified for the transaction to proceed.

If $\text{ethereum}_{\text{balance}}$ is greater than or equal to $\text{threshold}_{\text{score}}$, then $\text{ethereum}_{\text{balance}} \leftarrow (\text{ethereum}_{\text{balance}} - \text{threshold}_{\text{score}})$ operation is performed. If the $\text{ethereum}_{\text{balance}}$ is found to be insufficient, the operation is omitted, and a message is sent to the Credential Authority stating that the $\text{ethereum}_{\text{balance}}$ is insufficient.

Algorithm 2	**Identification of the Credential Holder and Credential Authority, as well as the Block Development Algorithm**
Input	Password, Name, Name of Authority, CF, EV, $\text{ethereum}_{\text{balance}}$
Output	Unique ID to Credential Authority(CA)User, EV, Block Development
Step1	Credential Authority (CA): User credentials are provided, including Password, Name, and Authority Name.
Step2	$\text{Application}_{\text{info}}$ ← Name(Credential Authority(CA)User)‖Password(Credential Authority(CA)U
Step 3	Verification of data
	If (integrity($\text{Application}_{\text{info}}$) == True) then
	Issue Unique ID
	Else
	Request declined
Step 4	If Credential Authority(CA)
	Submits the authorities' information (CF)

Step 5	Check $\text{ethereum}_{\text{balance}}$
	If $\text{ethereum}_{\text{balance}}$ is greater than or equal to $\text{threshold}_{\text{score}}$, then
	block[k] is developed
	Else
	block not developed
Step 6	$\text{ethereum}_{\text{balance}} \leftarrow (\text{ethereum}_{\text{balance}} - \text{threshold}_{\text{score}})$
Step 7	Information stored in a developed block
	$\text{block[k]} \leftarrow \text{DEV}_{\text{id}}/\ \text{G(EV)}$
	InterPlanetary file system $\leftarrow$ EV

Algorithm 3, given below, depicts the process by which the Certificate Issuing Authorities grant the certificate to the Credential Holder via $Cer_{issue}()$, and the validation performed using $Cer_{val}()$. The required certificate details need to be provided by the Credential Holder, $C_{ategory}$ (ER) $(Undergraduate\ or\ Postgraduate)$, Issuing authority (IA), name of the person received from the authority, and date. Also, authorized personnel from the certificate-issuing authority verify the information by storing it in the database $(valid(details) == True\ \&\&\ Present_{systemDB})$. Once the verification procedure is complete, the certificate is encrypted and then sent to the blockchain for the development of an Identification. For any operation to occur on the blockchain, MetaMask must have a balance. During validation, the Credential HolderId inputs are considered, and the details are verified to match whether they are stored in the blockchain $((ID == True))$. If the Credential Holder is valid, then true; otherwise, declined.

Algorithm 3	**$\text{Cer}_{\text{issue}}()$ and Cer_{val} () Algorithm**
Input	$\text{Cer}_{\text{category}}$, $\text{Cer}_{\text{issuer}}$, ID, Name, Date, Name of person who received certificate, $\text{Cer}_{\text{reciever}}$
Output	Issued Details of certificate
Step1	The details of Credential Authority are verified
	If $(\text{valid(details)} == \text{True}\ \&\&\ \text{Present}_{\text{systemDB}})$
	$\text{Ciphered}_{\text{cer}}(\text{EV}) \leftarrow \text{G}(\text{exist}_{\text{cer}})$
	If $(\text{valid(details)} == \text{True}\ \&\&\ \text{Presentnew}_{\text{systemDB}})$
	Details stored in local Database
	Process transferred to the blockchain network
Step2	Linked with MetaMask

Step 3	If request of MetaMask confirmed
	If connection established, procedure to next step. If not, exit
Step 4	If $\text{ethereum}_{\text{balance}}$ is greater than or equal to $\text{operation}_{\text{bal}}$ then
	Details set on blockchain
	Unique DEV_{id} given to certificate
	Else
	Less $\text{ethereum}_{\text{balance}}$, unable to generate DEV_{id}.
Step 5	The information received is decrypted from the InterPlanetary File System of $\text{DEV}_{\text{id.}}$
	Authority info ← info(InterPlanetary file system)
Step 6	Name and ID entered in the web application
Step 7	If Cer_{val} (ID is valid) then
	Verified successfully
	Else
	Invalid, Credential Holder request declined

EduVeriChain Revocation Authority (ERA)

The EduVeriChain Revocation Authority (ERA) is a crucial component of EduVeriChain, designed to securely and efficiently revoke academic credentials when they become invalid. Leveraging the Credential Revocation Authority (CRA) and Credential Status Enforcer (CSE) smart contracts, this module will enable EduVeriChain to automate credential revocation, thereby enhancing security, reducing operational overhead, and building trust in the credential verification system.

The EduVeriChain Revocation Authority (ERA) consists of two key smart contract modules:

- Credential Revocation Authority (CRA): Defines the specific conditions and roles for initiating the revocation process.
- Credential Status Enforcer (CSE): Enforces the rules set by the Credential Revocation Authority (CRA), performs the revocation, and maintains the integrity of the blockchain.

The goal is to ensure that credentials are revoked promptly and only by authorized entities, providing a transparent and secure process for managing credential lifecycle changes.

Credential Revocation Authority (CRA) Smart Contract

The Credential Revocation Authority (CRA) smart contract defines and enforces the policies governing when a credential can be revoked. It ensures that the revocation process follows strict guidelines to prevent unauthorized actions. Key Functionalities of the Credential Revocation Authority (CRA):

1. Authorized Nodes:
    - A list of nodes, called the authority-list, is maintained within the smart contract. These nodes represent trusted entities such as the accreditation body and participating universities.
    - Only nodes present in the authority list are permitted to initiate the credential revocation process.

2. Multi-Party Approval:
    - The Credential Revocation Authority (CRA) requires multi-signature approval from at least two distinct nodes on the authority list before proceeding with revocation.
    - This multi-party approval mechanism ensures that revocation cannot be executed by a single individual or entity, mitigating risks of insider threats or accidental revocation.
3. Revocation Policies:
    - Policies are defined to manage how and when a credential can be revoked, such as:
        - Credential expiration.
        - Detection of fraud or irregularities.
        - Accreditation body request.
    - The smart contract checks these policies before proceeding to the next phase.

Credential Status Enforcer (CSE)

The Credential Status Enforcer (CSE) smart contract executes the actual revocation once all predefined rules have been met. Key Functionalities of the Credential Status Enforcer (CSE):

1. Credential Revocation Execution:
    - The Credential Status Enforcer (CSE) verifies that the credential to be revoked is valid and matches the details in the blockchain.

- It then adds the credential to the on-chain Credential Revocation list.

2. Credential Revocation Counter:
    - The Credential Revocation counter tracks the number of authorities that have signed the revocation request. A credential can be revoked only after the required count is met.
    - A process-hash is generated when the first node signs the revocation request, and the counter is incremented each time another authority signs.
3. Batch Credential Revocation:
    - In case of systemic issues, such as the discovery of fraudulent credentials affecting an entire cohort, batch Credential Revocation is supported.
    - A batch_Merkle_root can be provided for batch operations, allowing bulk credential revocation while maintaining transparency.

Workflow of EduVeriChain Revocation Authority (ERA)

1. Revocation Request Initiation:
    - The revocation process is initiated by a university or accreditation body by calling the initiateRevocation() function in the Credential Revocation Authority (CRA).
    - The request must then be signed by at least one additional node on the authority list for it to proceed.
2. Verification by Credential Status Enforcer (CSE):
    - The Credential Status Enforcer (CSE) verifies the request using the revocation counter and the process-hash. It ensures that all necessary conditions are met, including multi-party approval.
3. Adding to Revocation List:
    - Upon successful validation, the Credential Status Enforcer (CSE) adds the credential to the revocation list. This status is recorded immutably on the blockchain.
    - The credentialId of the revoked certificate is mapped to true in the revokedCredentials mapping, ensuring that any verification query returns the credential as invalid.
4. Revocation Verification:
    - During credential verification, the Verification Smart Contract will check the revokedCredentials mapping to see if a credential has been revoked.

- If revoked, the verification function will return an error indicating that the credential is no longer valid.

5. Batch Revocation Support
    - The Credential Status Enforcer (CSE) supports batch revocation by utilizing a Merkle Tree structure to validate the entire batch of credentials.
    - The batch_Merkle_root is submitted to the Credential Status Enforcer (CSE) for validation, and all credentials under this root are revoked.
    - This approach significantly reduces the data on-chain and ensures a more efficient revocation process when systemic issues arise.

EduVeriChain Secure Decryption (ESD)

When a request is sent for the Accessing certificate () of a file by either the Credential Authority or the Credential Holder, the EduVeriChain system extracts the encrypted file, denoted as $G(Exe_{cer})$, from the InterPlanetary file system.

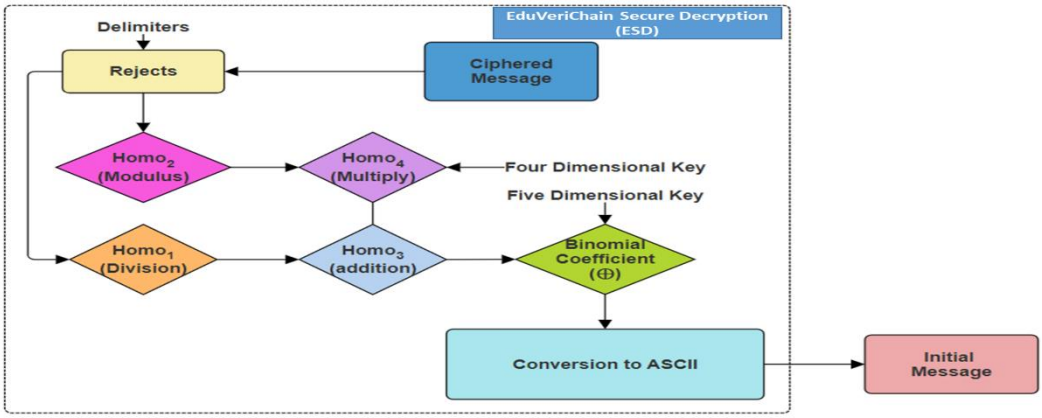

Figure 3. Process of EduVeriChain Secure Decryption (ESD)

If authorized correctly, the EduVeriChain Secure Decryption (ESD) $algorithm\ decrypt$s the encrypted information back to its original readable form. This phase allows Credential Holders requesting the Access Certificate file to read and understand it securely.

Algorithm 4 below describes the decryption process, using the ciphered data EV as input. This is also shown in Figure 3, where the process of EduVeriChain Secure Decryption (ESD) includes retrieving the number between h and $G_l \leftarrow EP_v[h_l : t_l]$ and then extracting another number post t between t and $TG_l \leftarrow EP_v[t_l : h_{l+1}]$. The five-dimensional secret keys are used: $\left(R_u \rightarrow \{R_{u0}, R_{u1}, \ldots, R_{u(p-1)}\}\right)$ for computation; FE_param_3 and FE_param_4 are used for multiplication and addition operations on the retrieved information, respectively. At the same time, using the four-dimensional secret keys $(V_u \rightarrow \{V_{u0}, V_{u1}, \ldots, V_{u(p-1)}\})$ for the operation

of Combinatorial Factor being performed on the information that results. The initial data are obtained by converting the ASCII scores and combining them.

Algorithm 4	**EduVeriChain Secure Decryption (ESD) Algorithm**
Input	Ciphered Data
Output	Initial Data
Step1	The Ciphered data is read as
	EV
Step2	Production of keys is done at random
	Four-dimensional Secret key $V_u \rightarrow (V_{u0}, V_{u1}, \dots, V_{u(p-1)})$
	Five-dimensional Secret key $R_u \rightarrow (R_{u0}, R_{u1}, \dots, R_{u(p-1)}$
Step 3	For $l = 0$ to $p - 1$ do till step 7
Step 4	Retrieve the substring between h_l, t_l, and t_l, h_{l+1}, implying
	$G_l \leftarrow EP_v[h_l : t_l]$
	$TG_l \leftarrow EP_v[t_l : h_{l+1}]$
Step 5	The operations FE_param_1, FE_param_2 are applied
	$FE\_param_3 : F_l \leftarrow multiplication(G_l,\ R_{ul})$
	$FE\_param_4 : U_l \leftarrow addition(F_l,\ TG_l)$
Step 6	Combinatorial Factor is implemented and changed into the internal data
	$BinoCoeff_l \leftarrow U_l \oplus V_{ul}$
	$E_l \leftarrow Initial(BinoCoeff_l)$
Step 7	Combine the results
	$E_v \leftarrow concatenate(E_l)$
Step 8	The resulting data, being the initial data, is retrieved $from\ E_v$

In this EduVeriChain system, we observe transactions in which the Credential Authority can perform operations such as storing information and accessing a certificate. In contrast, the Credential Holder can only view the information that is already stored. First, the Credential Authority enters the details of the certificate-issuing authority into the application. A unique ID is generated, and the information is then encrypted. Further, the ciphered data is sent to the computers linked to the InterPlanetary File System, where the hash scores are kept for EV. The related hash scores are stored on the blockchain if there is $sufficient\ ETH\ balance$ in MetaMask. The person who wishes to access the information should have an adequate

$Ethereum_{balance}$, and the related information encrypted with the hash score is decrypted. In conclusion, the information is shown to the Credential Holder in the application.

Performance Evaluation

The proposed approach, EduVeriChain, leverages blockchain and smart contracts for secure academic credential verification. It uses the InterPlanetary File System (IPFS) for decentralized storage, ensuring data immutability and preventing forgery. EduVeriChain incorporates automated credential issuance, verification, and revocation, using encryption to maintain data privacy. This approach enhances transparency, trust, and efficiency in managing academic records.

Table 1. ETH

Certificates	ETH Value
2	0.05
4	1.2
6	2.8
8	4.5
10	6
12	8.5

The graph shows a clear linear relationship between the **number of certificates** and the **ETH value** required in EduVeriChain. As the number of certificates increases from **2 to 12**, the ETH value rises from **0.1 to 18.6** ETH. This indicates a predictable increase in transaction costs for blockchain transactions, as each certificate issued or verified incurs a gas fee. The steady rise in ETH value highlights the cumulative cost of blockchain operations, which scales proportionally with the number of certificates managed. This trend is crucial for institutions planning to adopt blockchain technology, as it helps them anticipate costs as their certificate issuance grows.

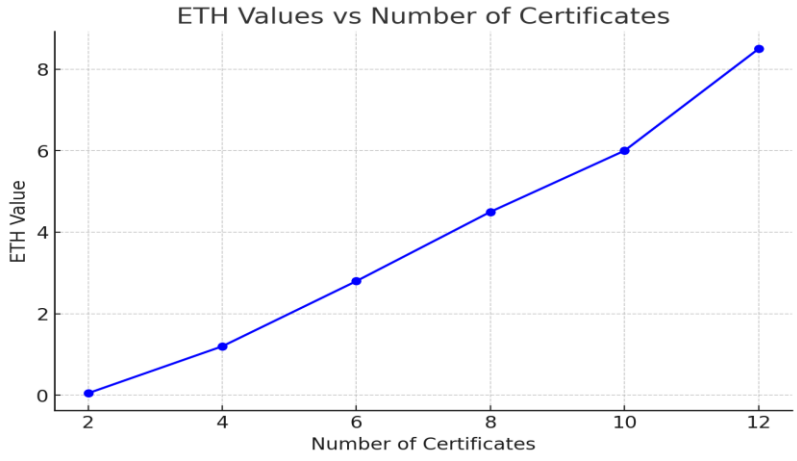

Figure 4. ETH for various certificate values

Results

The evaluation of EduVeriChain demonstrates its efficiency and scalability in academic credential management. The encryption time for EduVeriChain Secure Encryption (ESE) increases linearly with the number of certificates, maintaining low latency, indicating the system's capacity to handle multiple credentials concurrently. The storage time on the blockchain also increases linearly, reflecting efficient handling of additional data without creating significant computational burdens. Throughput analysis reveals that the system scales effectively with increasing transaction load while maintaining a satisfactory transaction rate per second (TPS). However, latency does increase with more transactions, though it remains within acceptable limits for document verification tasks.

EduVeriChain Secure Encryption (ESE)

Table 2. EduVeriChain Secure Encryption (ESE)

No of Certificates	EduVeriChain Secure Encryption (ESE) Time (ms)
1	0.0005
2	0.001
4	0.0025
8	0.005
16	0.01
18	0.012

The graph shows the relationship between the number of certificates and the EduVeriChain Secure Encryption (ESE) time in the EduVeriChain system. As the number of certificates increases from 1 to 18, the EduVeriChain Secure Encryption (ESE) time increases linearly, indicating that more certificates require additional computational resources for EduVeriChain Secure Encryption (ESE). For 1 certificate, the EduVeriChain Secure Encryption (ESE) time is 0.0005 ms; for 18 certificates, it increases to 0.012 ms. The data points—1, 2, 4, 8, 16, and 18 certificates—highlight that the EduVeriChain Secure Encryption (ESE) time grows steadily, showing the scalability of the EduVeriChain Secure Encryption (ESE) process. This linear trend suggests that the system can handle increasing workloads efficiently, though the increase in computational time must be accounted for as the number of certificates scales up. The EduVeriChain Secure Encryption (ESE) process, while increasing with the number of certificates, remains relatively low in time (measured in milliseconds), indicating that the system is efficient in encrypting multiple certificates concurrently.

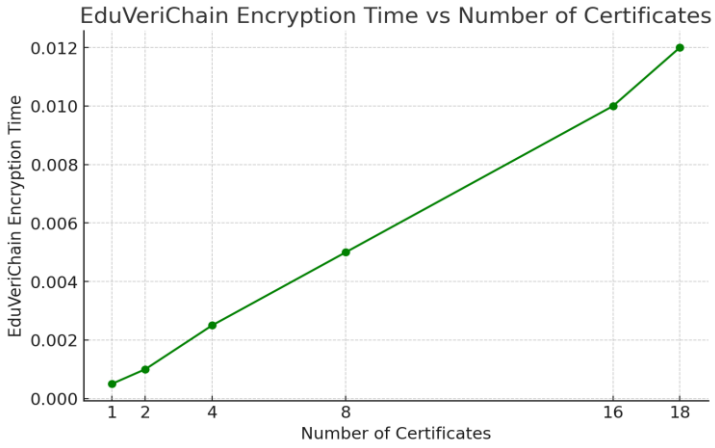

Figure 5. Eduverichain secure encryption time

Eduverichain Storage time

The graph illustrates the blockchain storage time required for different numbers of certificates in the EduVeriChain system. As the number of certificates increases from 1 to 18, the storage time also increases linearly, reflecting the additional time required to store more data on the blockchain. For 1 certificate, the blockchain storage time is 0.0001 ms, and for 18 certificates, it rises to 0.0035 ms. The plotted points for 1, 2, 4, 8, 16, and 18 certificates indicate consistent growth in storage time, as expected due to the additional blockchain operations required to securely and immutably store data. The increase in storage time is minimal, indicating that the system's blockchain-based storage mechanism is highly efficient. Even with 18 certificates, the storage time is below 0.004 ms, demonstrating that the storage process imposes a negligible computational burden, which is crucial for real-time applications in academic certificate management.

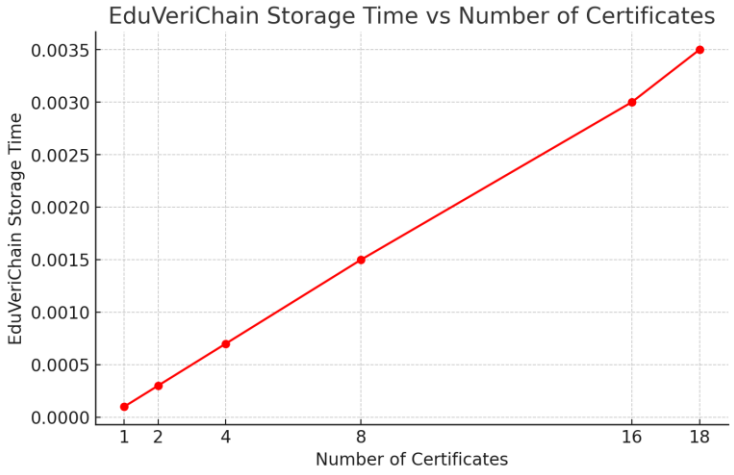

Figure 6. Eduverichain Storage time

Throughput

Throughput is the rate at which a system processes requests or completes tasks within a given time frame. In the context of blockchain-based systems, throughput is typically measured in **Transactions Per Second (TPS)**, which indicates the number of successful transactions a network can handle per second. High throughput is crucial for ensuring the system can efficiently manage multiple operations simultaneously, especially during peak usage, thereby improving scalability and overall performance.

Table 3. Docuverichain throughput comparison

No of Transactions	Throughput
5	2.5
10	3.8
15	4.9
20	5.5
25	6.2

The graph represents the relationship between the number of transactions and throughput for the DocVerifChain system. As the number of transactions increases from 5 to 25, the throughput also increases, indicating improved system performance.

- For **5 transactions**, the throughput is **2.5 TPS (Transactions Per Second)**, while for **25 transactions**, it reaches **6.2 TPS**.
- The upward trend in throughput indicates that DocVerifChain scales effectively, maintaining higher efficiency as transaction volume increases.

This demonstrates that DocVerifChain efficiently handles a larger volume of certificate verifications, ensuring scalability and reliability as the number of transactions grows.

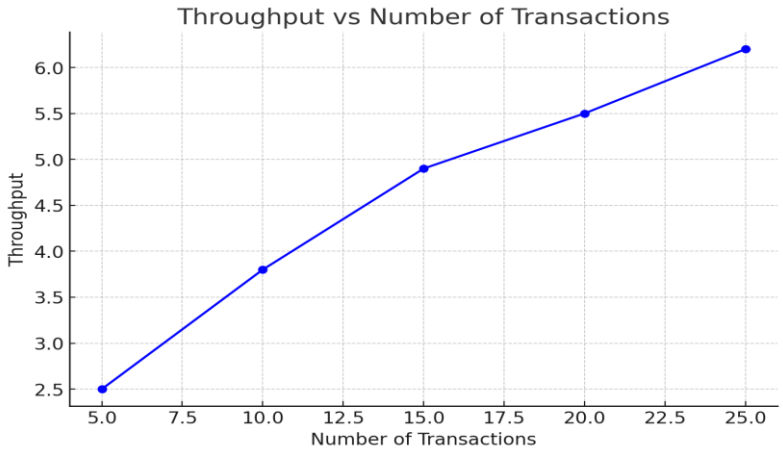

Figure 7. Throughput

Latency

Latency is the time delay between the initiation of a request and the completion of the response. In blockchain-based systems, latency is the time it takes for a transaction to be processed and confirmed on the network. Lower latency means faster transaction completion, which is essential for improving the responsiveness and user experience of systems that require real-time or near-real-time operations, such as academic credential verification in EduVeriChain.

Table 4. Docuverichain Latency

No of Transactions	Avg Latency (s)
5	15
10	18.5
15	22
20	30
25	35

The table and graph show the Average Latency for different numbers of transactions in the DocVerifChain system:

- The average latency starts at 15.0 seconds for 5 transactions and increases to 35.0 seconds for 25 transactions.
- The graph demonstrates a steady increase in latency with the number of transactions, reflecting the growing time required as the system handles more transactions.

This updated latency data suggests improved efficiency compared to previous values, maintaining lower latency and making DocVerifChain scalable for document verification tasks.

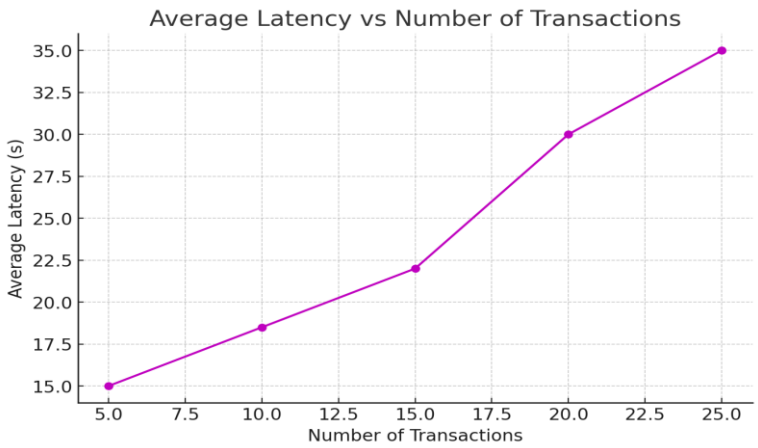

Figure 8. Latency

Comparative Analysis

- **51% Attack Resistance**:

- EduVeriChain utilizes Observer Nodes and decentralized consensus to protect against 51% attacks, ensuring that no single entity or group can gain control over the network.
- BlockMEDC remains potentially vulnerable to such an attack, as it lacks additional decentralization measures to counteract network dominance.

- **Eclipse Attack Resistance**:

- In EduVeriChain, the combination of Observer Nodes and the Credential Revocation Authority (CRA) enhances the network's defense against Eclipse attacks by ensuring node diversity and independent validation.
- BlockMEDC does not explicitly address Eclipse attacks, which makes it more susceptible to attackers isolating parts of the network.

- **Sybil Attack Resistance**:

- EduVeriChain is resistant to Sybil attacks by leveraging Observer Nodes and a robust identity verification process. These mechanisms prevent attackers from creating multiple fake nodes to compromise the network.
- BlockMEDC lacks explicit measures to counter Sybil attacks, increasing its vulnerability to identity spoofing and network compromise.

- **Automated Revocation**:

- EduVeriChain employs a robust Credential Revocation Authority (CRA) and Credential Status Enforcer (CSE) to automate the revocation process, including multi-signature approval, which enhances security against unauthorized revocations.
- BlockMEDC also supports on-chain revocation, but it does not provide the same level of automation and multi-signature enforcement as EduVeriChain.

Table 5. Comparison

Security Property	EduVeriChain	BlockMEDC
51% Attack	Resistant (Decentralized Nodes)	Potentially Vulnerable
Eclipse Attack	Resistant (Nodes and CRA)	Not Explicitly Addressed
Sybil Attack	Resistant (Observer Nodes, Identity Verification)	Not Explicitly Addressed
Automated Revocation	Automated via CRA and CSE	On-Chain Revocation

Conclusion

EduVeriChain offers an innovative blockchain-based solution for the secure issuance, verification, and management of academic credentials. By leveraging smart contracts, decentralized storage via IPFS, and robust encryption techniques, the proposed system addresses significant challenges in the current academic verification landscape, including credential fraud, inefficiencies, and reliance on centralized authorities. The use of EduVeriChain Secure Encryption (ESE) and the Credential Revocation Authority (CRA) ensures both data privacy and an effective revocation process, enhancing the reliability of the verification mechanism. Performance evaluation demonstrates that EduVeriChain maintains high throughput, low latency, and predictable costs, making it a scalable and efficient solution suitable for real-world deployment in academic institutions. This work paves the way for more trustworthy, globally adaptable academic credential management, significantly contributing to the fight against credential forgery and promoting trust in digital education systems.

Acknowledgement

I sincerely thank my supervisor, Dr. Ashok Kumar T A, Professor and Director in the School of Science and Computer Studies, CMR University, for their continuous guidance and immense support. All the related and referenced articles are cited and acknowledged appropriately. I thank my family and friends for helping to overcome the difficulties I faced while writing the manuscript.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the authors have witnessed ethical issues including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancy.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alam, G. M. (2021). Does online technology provide sustainable HE or aggravate diploma disease? Evidence from Bangladesh—A comparison of conditions before and during COVID-19. *Technology in Society*, *66*, 101677.

Ayub Khan, A., Laghari, A. A., Shaikh, A. A., Bourouis, S., Mamlouk, A. M., & Alshazly, H. (2021). Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Applied Sciences*, *11*(22), 10917.

Bajwa, N. K. (2018). *Modelling and simulation of blockchain based education system* (Doctoral dissertation, Concordia University).

Bautista, M. M., & Comendador, B. E. V. (2016). Adoption of an Open Source Optical Character Recognition (OCR) for Database Buildup of the Students' Scholastic Records. *International Journal of Information and Electronics Engineering*, *6*(3), 206.

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2021). Blockchain in education management: present and future applications. *Interactive Technology and Smart Education*, *18*(1), 1-17.

Diaz-Infante, N., Lazar, M., Ram, S., & Ray, A. (2022). Demand for online education is growing. Are providers ready. McKinsey & Company, 20.

Durant, E., & Trachy, A. (2017). Digital Diploma debuts at MIT. *Massachusetts Institute of Technology*.

Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2025). Blockmedc: Blockchain smart contracts for securing moroccan higher education digital certificates. *IEEE Access*.

Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2025). Blockmedc: Blockchain smart contracts for securing moroccan higher education digital certificates. *IEEE Access*.

Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2025). Blockmedc: Blockchain smart contracts for securing moroccan higher education digital certificates. *IEEE Access*.

Han, M., Li, Z., He, J., Wu, D., Xie, Y., & Baba, A. (2018, September). A novel blockchain-based education records verification solution. In *Proceedings of the 19th annual SIG conference on information technology education* (pp. 178-183).

Hope, J. (2018). Issue secure digital credentials using technology behind bitcoin. *The Successful Registrar*, *17*(11), 1-4.

Kim, S. K. (2022). Blockchain smart contract to prevent forgery of degree certificates: artificial intelligence consensus algorithm. *Electronics*, *11*(14), 2112.

Kim, S. K. (2022). Blockchain smart contract to prevent forgery of degree certificates: artificial intelligence consensus algorithm. *Electronics*, *11*(14), 2112.

Kwok, A. O., & Treiblmaier, H. (2022). No one left behind in education: blockchain-based transformation and its potential for social inclusion. *Asia Pacific Education Review*, *23*(3), 445-455. doi: 10.1007/s12564-021-09735-4.

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.

Mahlaba, J., Mishra, A. K., Puthal, D., & Sharma, P. K. (2022). Blockchain-based sensitive document storage to mitigate corruptions. *IEEE Transactions on Engineering Management*, *71*, 12635-12647.

Mahlaba, James, Amit Kumar Mishra, Deepak Puthal, and Pradip Kumar Sharma. "Blockchain-based sensitive document storage to mitigate corruptions." *IEEE Transactions on Engineering Management* 71 (2022): 12635-12647.

Palma, L. M., Vigil, M. A., Pereira, F. L., & Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in Brazil. *International Journal of Network Management*, *29*(3), e2061.

Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Mumtaz, S., & ul Qayyum, Z. (2020). Docschain: Blockchain-based IoT solution for verification of degree documents. *IEEE Transactions on Computational Social Systems*, *7*(3), 827-837.

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. *Ieee Access*, *11*, 64679-64696.

Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. *Journal of critical reviews*.

Savelyeva, T., & Park, J. (2022). Blockchain technology for sustainable education. *British Journal of Educational Technology*, *53*(6), 1591-1604. doi: 10.1111/bjet.13273.

Schmidt, P. (2016). Blockcerts—an open infrastructure for academic credentials on the blockchain. *MLLearning (24/10/2016)*.

Xie, R., Wang, Y., Tan, M., Zhu, W., Yang, Z., Wu, J., & Jeon, G. (2020). Ethereum-blockchain-based technology of decentralized smart contract certificate system. *IEEE Internet of Things Magazine*, *3*(2), 44-50.

Bibliographic information of this paper for citing:

D V, Sheela & T A, Ashok Kumar (2026). EduVeriChain: A Blockchain-Based System for Secure Academic Credential Verification and Management. *Journal of Information Technology Management*, 18 (1), 158-183. https://doi.org/10.22059/jitm.2026.106536